Length Bounds for the Conjugacy Search Problem in Relatively Hyperbolic Groups, Limit Groups and Residually Free Groups

Zoe Ann O'Connor

Submitted for the degree of
Doctor of Philosophy

Heriot-Watt University

Department of Mathematics,
School of Mathematical and Computer Sciences.

February 11, 2014

Abstract

In this thesis we prove conjugacy length bounds for several classes of groups. We use geometric and algebraic methods to show that there is a polynomial conjugacy length bound for relatively hyperbolic groups, a linear multiple conjugacy length bound for limit groups, and a polynomial multiple conjugacy length bound for finitely presented residually free groups.

In loving memory of my father,
Richard John O'Connor
2 June 1957 - 20 May 2013

This work could not have been completed without the unwavering support and encouragement provided by my father. Through his own success from humble roots, he showed me how my goals can be attained by hard work and perseverance.

Acknowledgements

Special thanks to my supervisor, Prof. Jim Howie, for his patience and guidance over the last four years.

Thanks to all my friends and family who have given me their support.

I am grateful to the Engineering and Physical Sciences Research Council (EPSRC), whose Doctoral Training Grant funded this thesis.

List of Figures

Contents

Chapter 1

Introduction

1.1 Motivation

A *decision problem* is a question which has a *yes* or *no* answer. A decision problem is called *decidable* for a particular class of inputs if there exists an effective method which will provide a yes or no answer for that class of inputs. In 1911 Max Dehn introduced three decision problems: The isomorphism problem, the word problem and the conjugacy problem [21]. The *conjugacy problem* is of relevance to this thesis, and is described below. A natural extension of the conjugacy problem is the *conjugacy search problem*, which is not a decision problem since it is not a yes/no question – rather, the focus is on finding an unknown group element which satisfies the specified condition. Finally, this problem can be made more difficult by introducing a conjugate pair of *lists* of elements.

Problem 1.1.1. Conjugacy problem

Given two elements a, b in a group G, is there some $x \in G$ such that $x^{-1}ax = b$?

Problem 1.1.2. Conjugacy search problem

Given two elements a, b in a group G such that a is conjugate to b, find an element $x \in G$ such that $x^{-1}ax = b$.

Problem 1.1.3. Multiple conjugacy search problem

Given two lists $A = [a_i]_{i \in I}, B = [b_i]_{i \in I}$ of elements a, b in a group G, such that a_i is conjugate to b_i in G for all i, find an element $x \in G$ such that $x^{-1}a_i x = b_i$ for all i.

These problems are relevant to group-based public key cryptography. Public key cryptography is used to securely send encrypted messages between two parties over a public channel (such as the internet, or the postal system), without a third party being able to decrypt or understand the message. This is incredibly useful in modern times, since so much communication and commerce is conducted over the internet,

and without a secure way of encrypting information such as bank account details, transactions such as e-commerce, online banking, and so on would be unfeasible.

A real-world example of public key cryptography which is worthy of mention is RSA cryptography, named after its inventors Rivest, Shamir and Adleman. Without going off-topic with too much detail, the essence of RSA is using private information (two large prime numbers) to generate a public key (the product of these two primes), and the most naïve approach to "cracking" the encryption is to try to factorise the product. The strength of this system lies in the amount of computational time it takes to factorise numbers with such large factors. One drawback of this scheme is the relative difficulty in discovering large prime numbers (and proving that they are prime!) In practice, RSA is used for authentication and to exchange cryptographic keys, since it is much slower than other current methods of public key encryption. The reader is referred to [18] for more information on RSA cryptography.

A key agreement protocol is a method of establishing a shared private key to decrypt a message which has been encrypted by public keys and sent over a public channel. Several key agreement protocols have been proposed [2, 35] which are based on the original Diffie-Hellman protocol which was developed in 1976 [22]. The following example of group-based public key cryptography is due to Anschel, Anschel and Goldfeld [2]:

The group G and two subgroups of G

$$S_A = \langle s_1, s_2, \ldots, s_n \rangle$$

$$S_B = \langle t_1, t_2, \ldots, t_n \rangle \tag{1.1}$$

are made publicly available. Suppose Alice and Bob want to agree on a private shared key. Alice has a private key $a \in S_A$, and publishes a public key in the form of a list of elements:

$$L_A = [a^{-1}t_1a, \ldots, a^{-1}t_na]. \tag{1.2}$$

Bob has a private key $b \in S_B$ and similarly publishes a public key

$$L_B = [b^{-1}s_1b, \ldots, b^{-1}s_nb]. \tag{1.3}$$

Since Alice can form $b^{-1}ab$ from L_B and Bob can form $a^{-1}ba$ from L_A then the private shared key is the element $a^{-1}b^{-1}ab$. Someone eavesdropping on the communications could find a and b from the publicly available information by finding the solution to the multiple conjugacy search problem on S_B and L_A, and S_A and L_B respectively. Hence it is important that for the chosen group, the multiple conjugacy search problem is difficult to solve.

Another application of the conjugacy search problem is its link to differential

geometry: free homotopy classes of loops in compact non-positively (or negatively) curved spaces correspond to conjugacy classes in CAT(0) (or hyperbolic) groups.

Definition 1.1.4. Let (X, d) be a geodesic metric space (see Definition 2.2.3). It is a *CAT(0) space* if for any geodesic triangle Δ and $x, y \in \Delta$ we have

$$d(x, y) \leq d(\overline{x}, \overline{y}), \tag{1.4}$$

where $\overline{x}, \overline{y}$ are the corresponding points in the comparison triangle $\overline{\Delta} \subset \mathbb{R}^2$.

A group which acts properly, cocompactly and isometrically on a CAT(0) space is called a *CAT(0) group*.

Determining whether two elements are conjugate corresponds to the problem of determining whether two loops are freely homotopic. Furthermore, finding an upper bound for the width of geodesic homotopies can provide an upper bound on the length of an element which conjugates two lists of elements and vice versa. Kokarev's paper [36] is an example of this. It is worth noting that limit groups, the subject of Chapter 4, are CAT(0). [1]

Group theorists have been examining the conjugacy search problem for different families of groups. Is there an upper bound we can impose on the geodesic length of such an element x? This was the strategy proposed by Hughes and Tannenbaum [29] for *length-based attacks* on cryptosystems based on the word/conjugacy problems. We define a length function for the conjugacy search problem as follows:

Definition 1.1.5. Let G be a group with a conjugate to b in G. A *conjugacy length bound* on G with respect to a and b is a function $f : \mathbb{N} \to \mathbb{N}$ such that there is an element x which conjugates a to b: $x^{-1}ax = b$ and

$$\|x\|_g \leq f(\max\{\|a\|_G, \|b\|_G\}). \tag{1.5}$$

Similarly we define a length function for the multiple conjugacy search problem:

Definition 1.1.6. Let G be a group with two lists of elements

$$A = [a_1, \ldots, a_n],$$

$$B = [b_1, \ldots, b_n] \tag{1.6}$$

such that a_i is conjugate to b_i in G for $i = 1, \ldots, n$. A *multiple conjugacy length bound* on G with respect to A and B is a function $f : \mathbb{N} \to \mathbb{N}$ such that there is an element x which conjugates a_i to b_i for all i: $x^{-1}a_ix = b_i$ for $i = 1, \ldots, n$ and

$$\|x\|_g \leq f(\max\{\|a_i\|_G, \|b_i\|_G\}_{i=1}^n). \tag{1.7}$$

Note that, for $k > 1$, a function of the L_∞-norm (that is, $f(\max\{n_i\}_{i=1}^k)$ for $n_i \in \mathbb{Z}$) is asymptotically equivalent to a function of the L_1-norm (that is, $f(\sum_{i=1}^k n_i)$ for $n_i \in \mathbb{Z}$):

$$k \cdot f(\max\{n_i\}_{i=1}^k) \geq f\left(\sum_{i=1}^k n_i\right) \tag{1.8}$$

and, for $k > 1$,

$$f(\max\{n_i\}_{i=1}^k) < f\left(\sum_{i=1}^k n_i\right). \tag{1.9}$$

The aim of this thesis is to investigate the conjugacy search problem and multiple conjugacy search problem for various related families of groups. For each of these families of groups we find an upper length bound, for a minimal-length conjugating element, as a function of the input (conjugate) elements.

1.2 Existing results for similar problems

In this section we provide an overview of recent work regarding the conjugacy search problem in various families of groups.

For the conjugacy search problem in hyperbolic groups, Bridson and Haefliger [11] described an algorithm which gives a linear conjugacy length bound. Bridson and Howie showed [12] that the multiple conjugacy search problem also has a linear multiple conjugacy length bound. This paper goes further, presenting an algorithm which solves the multiple conjugacy search problem in at most quadratic time, provided at least one of the input elements is non-torsion. Buckley and Holt [15] have improved this result by creating an algorithm which runs in linear time and works in the case in which the lists contain no elements of infinite order.

Definition 1.2.1. A group G with finite generating set X is *automatic* if there is a regular language L over X which represents every element of G exactly once, and there is a set of multipliers corresponding to every $x \in X \cup \{1\}$ which accept a pair (w_1, w_2) of words $w_i \in L$ if and only if $w_1 x = w_2$ in G.

An automatic group is *biautomatic* if there are multipliers corresponding to both left and right multiplication.

Examples of automatic groups include finite groups, braid groups, and negatively curved groups. Hyperbolic groups and braid groups are biautomatic.

Epstein et. al. [23] asked if there are any automatic groups which have a decidable conjugacy problem. Gersten and Short [26] have shown that the conjugacy problem for biautomatic groups is recursively solvable. It is known that the conjugacy length function for biautomatic functions is at most exponential [11].

Definition 1.2.2. A *right-angled Artin group* is a group with a presentation of the form

$$\langle x_1, x_2, \ldots, x_n | (x_i x_j)^{M_{i,j}} = (x_j x_i)^{M_{i,j}} \rangle \tag{1.10}$$

where M is a symmetric matrix with zeros on the diagonal, and all other entries $M_{i,j} \in \{0, 1\}$.

Liu et. al. [38] presented an algorithm which solved the word and conjugacy problems in right-angled Artin groups (called "partially commutative monoids" in this paper) in linear time, a result which was proved by Crisp et. al. [19] using an alternative method. They also proved a linear bound for a family of CAT(0) subgroups of right-angled Artin groups. The paper by Kokarev [36] has shown that CAT(0) groups have an upper length bound for the multiple conjugacy search problem which is a linear function of the input elements, but is also dependent upon the conjugacy classes of the input elements.

In 2004 Bumagin published a method [16] to solve the conjugacy search problem for relatively hyperbolic groups, which was shown by Ji, Ogle and Ramsey in 2007 [30] to have a P-solvable conjugacy bound, for a polynomial P of degree $576n$, where n is the degree of polynomial bounding the conjugacy search problem for the peripheral subgroups of the relatively hyperbolic group G. We can do much better, as this thesis shows.

1.3 Main results in this thesis

In Chapter 3 we use results from Osin's book [46] to establish a polynomial length bound for conjugators for the conjugacy search problem in relatively hyperbolic groups. This is an improvement on the existing bound inferred from Bumagin's paper [16], which is also polynomial but of a much higher degree. Furthermore, we show that a section of Bumagin's paper is in fact unnecessary, since the cases she describes in this section cannot occur. (Remark 3.1.16)

Chapter 4 focuses on limit groups. The cubic conjugacy length bound on the conjugacy search problem in limit groups, implied by Chapter 3, is improved further to a linear length bound. It is also shown that the multiple conjugacy search problem for lists of any finite length can be simplified to the multiple conjugacy search problem for lists of length two, with a unique solution (provided the problem cannot be reduced to lists of one element). The multiple conjugacy length bound is shown to be linear - this is an improvement on Kokarev's work [36], as this new bound is independent of conjugacy classes.

Finally, in Chapter 5, by viewing finitely presented residually free groups as full subdirect products of finite sets of limit groups, we build on the previous chapter to

show that the multiple conjugacy search problem for such groups has a polynomial length bound.

Chapter 2

Background

In this chapter we introduce some of the topics and techniques required to prove the theorems in this thesis.

2.1 Bass-Serre theory

Bass-Serre theory will play an important role in this thesis. We review the fundamentals here and refer the reader to Serre's book [51] for details.

Definition 2.1.1. A *graph* X is a tuple $(V, E, \alpha, \omega, {}^{-})$ consisting of a nonempty set of vertices $V = V(X)$, a set of edges $E = E(X)$, and three maps

$$\alpha : E \to V, \quad \omega : E \to V, \quad {}^{-} : E \to E \tag{2.1}$$

where the map ${}^{-}$ is an involution such that $\overline{e} \neq e$, and $\alpha(e) = \omega(\overline{e})$ for every $e \in E$. The vertex $\alpha(e)$ is known as the *origin* of the edge e and the vertex $\omega(e)$ is known as the *terminus* of the edge e. The edge $\overline{e}$ is the *inverse* of the edge e. Two vertices v_1, v_2 are said to be *adjacent* if there is an edge $e \in E$ such that $v_1 = \alpha(e)$ and $v_2 = \omega(e)$.

Definition 2.1.2. Let X_1, X_2 be graphs. The map

$$\theta : V(X_1) \cup E(X_1) \to V(X_2) \cup E(X_2) \tag{2.2}$$

is a *homomorphism* if it is edge-preserving – that is, two vertices in X_2 are adjacent only if their preimages in X_1 are adjacent. We call the homomorphism θ an *isomorphism* if it is also bijective, and an automorphism if it is an isomorphism and $X_1 = X_2$.

Definition 2.1.3. A group G is said to *act* on a graph X if there is a map

$$\mu : G \times X \to X \tag{2.3}$$

such that

- For fixed $g \in G$, the induced map $g : X \to X$ is a graph automorphism of X,
- $1(x) = x$ for all $x \in X$,
- For any $g, h \in G$ and any $x \in X$, $g(h(x)) = (gh)(x)$.

This map is called the *group action*.

Definition 2.1.4. A group G is said to act *without inversions* on a graph X if for all $g \in G$ and $e \in E(X)$, $g(e) \neq \overline{e}$.

Definition 2.1.5. Let μ be the action of a group G on a graph X. For any $x \in X$, the set

$$\mathcal{O}(x) := \{g(x) \ : \ g \in G\} \tag{2.4}$$

is called the *orbit* of the element x.

Definition 2.1.6. Let μ be the action of a group G on a graph X. The *stabiliser* of $x \in X$ is the set

$$\mathrm{Stab}_G(x) := \{g \in G \ : \ g(x) = x\}. \tag{2.5}$$

Lemma 2.1.7. *Let G be a group acting on a graph X. If $g(u) = v$ for some $u, v \in V(X)$ and $g \in G$, then $Stab_G(u) = g^{-1} Stab_G(v) g$.*

The same is true for edge stabilisers: if $g(e_1) = e_2$ for some $e_1, e_2 \in E(X)$ and $g \in G$, then $\mathrm{Stab}_G(e_1) = g^{-1}\mathrm{Stab}_G(e_2)g$. Thus for any vertex or edge orbit $\mathcal{O}(x)$ we can associate a canonical subgroup $\mathrm{Stab}_G(x)$.

Definition 2.1.8. A *graph of groups* $\mathcal{G}(X, \Gamma)$ is a graph X and a set Γ of groups such that:

- Each $x \in X$ is associated with a group $G_x \in \Gamma$. These are called *vertex groups* when $x \in V(X)$ and *edge groups* when $x \in E(X)$,
- For each edge $e \in E(X)$ there is an embedding $\alpha_e : G_e \hookrightarrow G_{\alpha(e)}$.

Definition 2.1.9. Let $\mathcal{G}(X, \Gamma)$ be a graph of groups, and choose a maximal subtree T of X. Borrowing Serre's notation [51], let $F(G, X)$ be the quotient of the free product

$$F(G, X) = *_{v \in V(X)} G_v * \{t_e \ : \ e \in E(X)\} \tag{2.6}$$

by the normal subgroup generated by the elements

$$t_e t_{\overline{e}} \text{ and } t_e \alpha_e(g) t_e^{-1} (\alpha_{\overline{e}}(g))^{-1} \tag{2.7}$$

for all $e \in E(X)$, $g \in G_e$.

The *fundamental group* $\pi_1(\mathcal{G}(X,\Gamma))$ of the graph of groups $\mathcal{G}(X,\Gamma)$ with respect to the maximal subtree T is defined as the quotient of the group $F(X,\Gamma)$ by the normal closure of the elements t_e for all $e \in E(T)$.

It can be shown [51] that the fundamental group of a graph of groups does not depend on the choice of maximal subtree.

Definition 2.1.10. Let G be a group which acts on a graph X without inversions. The *quotient graph* of X by G, denoted $G\backslash X$ is the graph with vertex set $\{\mathcal{O}(v) : v \in V(X)\}$ and edge set $\{\mathcal{O}(e) : e \in E(X)\}$ with the following restrictions:

- $\alpha(\mathcal{O}(e)) = \mathcal{O}(v)$ if there is $u \in \mathcal{O}(v)$ such that $u = \alpha(e)$
- The inverse of $\mathcal{O}(e)$ is $\mathcal{O}(\overline{e})$

This graph is well-defined, since $\mathcal{O}(e) \neq \mathcal{O}(\overline{e})$ for all $e \in E(X)$.

Example 2.1.11. Suppose that $G\backslash X$ is a segment with vertices $\mathcal{O}(v_1)$ and $\mathcal{O}(v_2)$, and edge $\mathcal{O}(e)$ (with an inverse $\mathcal{O}(\overline{e})$). Then there are elements $u_1 \in \mathcal{O}(v_1)$ and $u_2 \in \mathcal{O}(v_2)$ and a lift to a segment of X with vertices u_1 and u_2. Without loss of generality we can assume that $v_1 = u_1$ and $v_2 = u_2$. So we can associate a graph of groups with vertex groups $G_{u_1} = \mathrm{Stab}_G(u_1)$, $G_{u_2} = \mathrm{Stab}_G(u_2)$ and $G_e = \mathrm{Stab}_G(e)$.

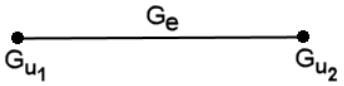

Figure 2.1: Illustration of Example 2.1.11

Definition 2.1.12. Let $G = \langle A \mid R \rangle$ and $H = \langle B \mid S \rangle$ be two groups containing subgroups $K_1 \leq G$, $K_2 \leq H$, such that $\phi : K_1 \to K_2$ is an isomorphism.

The free product of G and H amalgamated over the subgroup K_1, sometimes just called an *amalgamated free product*, is defined as follows:

$$G *_{K_1} H := \langle A \cup B \mid R \cup S, k = \phi(k) \forall k \in K_1 \rangle \tag{2.8}$$

The action of an amalgamated free product $G *_K H$ on a tree is bipartite. The corresponding fundamental domain F is a segment (two vertices joined by an edge). The vertices of this segment have stabilisers G and H, and the edge stabiliser is K.

Proposition 2.1.13 ([51]). *If X is a connected tree and $G\backslash X$ is a segment as in Example 2.1.11 then*

$$G \cong \ Stab(u_1) *_{Stab(e)} \ Stab(u_2). \tag{2.9}$$

The converse is also true: any group which is an amalgamated free product has a quotient graph which is a segment.

At this stage it is worth mentioning that certain amalgamated free products can also be viewed as HNN extensions.

Definition 2.1.14. Let $G = \langle A \mid R \rangle$, and let $\phi : H \to K$ be an isomorphism between two subgroups H, K of G. Let t be a new element not in G. The group defined by the presentation

$$G*_\phi := \langle A, t \mid R \cup \{t^{-1}h^{-1}t\phi(h),\ \forall h \in H\}\rangle, \tag{2.10}$$

is called the *HNN extension* of G with respect to ϕ. The new generator t is called the *stable letter*, and H, K are the *associated subgroups* of this HNN extension.

Hence, any amalgamated free product of the form

$$G = H *_{\langle w\rangle} (\langle w\rangle \times A_r), \tag{2.11}$$

in which H is any group, $w \in H$, and A_r is a free abelian group of rank r, can be viewed as a series of HNN extensions

$$H_{i+1} := \langle H_i, t_{i+1} \mid t_{i+1}^{-1} w^{-1} t_{i+1} w\rangle \tag{2.12}$$

for $i = 0, \ldots, r$, with $H_0 = H$ and $H_r = G$. This is also known as an iterated extension of centralisers. This structure is used in Chapter 4, but we do not make use of the equivalent HNN definition in this thesis.

Theorem 2.1.15 ([51]). *Let G be a group acting without inversions on a connected tree T, and let $X = G\backslash T$. Then there is a graph of groups $\mathcal{G}(X, \Gamma)$ such that for any maximal subtree S of X,*

$$G \cong \pi_1(\mathcal{G}(X, \Gamma), S). \tag{2.13}$$

Conversely, if G is the fundamental group $\pi_1(\mathcal{G}(X, \Gamma), S)$ of a graph of groups $\mathcal{G}(X, \Gamma)$ then there exists a connected tree T on which G acts without inversions, such that $G\backslash T \cong X$.

Definition 2.1.16. Let $\mathcal{G}(X, \Gamma)$ be a graph of groups. If G is isomorphic to the fundamental group of $\mathcal{G}$ then $\mathcal{G}$ is a *graph of groups decomposition* of G.

Definition 2.1.17. Let G be a group and $\mathcal{C}$ be a class of groups. A *$\mathcal{C}$-splitting* is a graph of groups decomposition of G in which every edge group is in $\mathcal{C}$.

2.2 Hyperbolic metric spaces, hyperbolic groups

Relatively hyperbolic groups benefit from the properties of hyperbolic metric spaces, so in this section we define a hyperbolic metric space and present a well-known lemma, called the Fellow Traveller Property, which will be useful later. Since relatively hyperbolic groups are a generalisation of Gromov hyperbolic groups, we define these in this section.

Definition 2.2.1. Let $M = (X, d)$ be a metric space, and let $x, y, z \in X$. The *Gromov product* of y and z with respect to x is

$$(y|z)_x = \frac{1}{2}(d(y, x) + d(z, x) - d(y, z)). \tag{2.14}$$

Definition 2.2.2. Let $\delta \geq 0$. A metric space $M = (X, d)$ is said to be (Gromov) *δ-hyperbolic* if

$$(x|z)_w \geq \min\{(x|y)_w, (y|z)_w\} - \delta \tag{2.15}$$

for all points w, x, y, z in M. If the value of δ is unimportant, then we can also say that M is *(Gromov) hyperbolic*.

An alternative definition of δ-hyperbolicity uses the idea of δ-slim geodesic triangles.

Definition 2.2.3. A *geodesic segment* between two points x, y in a metric space M is the image of an isometric embedding $\iota : [0, \ell] \to M$ with $\iota(0) = x$ and $\iota(\ell) = y$. We denote such a segment by $[x, y]$. A geodesic segment does not necessarily exist between two points, and if it does exist, it is not necessarily unique. If geodesic segments exist for all points in a metric space M, then M is called a *geodesic metric space*.

Definition 2.2.4. A *geodesic triangle* T with vertices $x, y, z \in M$ is the union of three geodesic segments $[x, y]$, $[y, z]$ and $[x, z]$. We say that T is *δ-slim* if each side of the triangle is contained within the δ-neighbourhood of the union of the other two sides.

Definition 2.2.5. Let M be a geodesic metric space. If there is some constant δ such that all triangles in M are δ-slim, then we say that M is a *δ-hyperbolic metric space*.

The two definitions of δ-hyperbolicity are equivalent, although a hyperbolic metric space would produce different values of δ depending on which definition is used. In this thesis we will use Definition 2.2.5.

Definition 2.2.6. Let G be a group with generating set X. The *Cayley graph* $\Gamma(G, X)$ is a graph for which each vertex is associated with a unique element $g \in G$, and for

every $g \in G$ and $x \in X$, the vertex corresponding to g is joined to the vertex gx by an edge which corresponds to the generator x. The edge set of G is therefore the set of pairs $\{(g, gx),\ g \in G,\ x \in X\}$.

We can view Cayley graphs as geodesic metric spaces. First, let G be a group with generating set X. Every element in the group can be written as a word in X:

$$g = x_1^{\varepsilon_1} x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n} \tag{2.16}$$

where $x_i \in X$ and $\varepsilon_i \in \{1, -1\}$ for all $i = 1 \ldots n$. The number n is the *length* of this word. We denote by $\|g\|_X$ the length of a smallest word in the generating set X representing g.

Definition 2.2.7. Given two elements $g_1, g_2 \in G$ we define $d_X(g_1, g_2)$ to be the length of the smallest word in X representing $g_1^{-1} g_2$. This is a metric on G, which we call the *word metric*.

The function d_X is dependent on the choice of generating set for G.

For a group G with generating set X and corresponding Cayley graph $\Gamma(G, X)$, the word metric on G with respect to X is consistent with the natural path metric on Γ: if the two points in question are vertices v_1 and v_2 of the graph, then the distance between these two points (by the natural path metric) is the length of a geodesic between these two points. This geodesic corresponds to a shortest word over the generating set X which represents $v_1^{-1} v_2$ in G.

Definition 2.2.8. Let G be a group with finite generating set X. If the Cayley graph $\Gamma(G, X)$ is δ-hyperbolic as a metric space, then G is called a δ-hyperbolic group.

Example 2.2.9.

1. Every finite group is hyperbolic, since its Cayley graph is finite.

2. The Cayley graph of a free group with respect to a basis is a tree. Trees are hyperbolic, since each side of any triangle is contained within the union of the other two sides.

Definition 2.2.10. Two connected graphs Γ_1, Γ_2 are *quasi-isometric* if there exist functions

$$\phi_1 : V(\Gamma_1) \to C(\Gamma_2), \quad \phi_2 : V(\Gamma_2) \to C(\Gamma_1) \tag{2.17}$$

and constants a, b, c, d such that for all $x_1, x_2 \in V(\Gamma_1)$ and for all $y_1, y_2 \in V(\Gamma_2)$, the following conditions hold:

- $d_1(\phi_2(y_1), \phi_2(y_2)) \leq a \cdot d_2(y_1, y_2)$

- $d_2(\phi_1(x_1), \phi_1(x_2)) \leq b \cdot d_1(x_1, x_2)$
- $d_1(\phi_2\phi_1(x_1), x_1) \leq c$
- $d_2(\phi_1\phi_2(y_1), y_1) \leq d$.

Lemma 2.2.11. *Fellow Traveller Property*

Let (X, d) be a δ-hyperbolic geodesic metric space, and let $\gamma_1 : [0, T_1] \to X$ and $\gamma_2 : [0, T_2] \to X$ be two geodesics such that $d(\gamma_1(0), \gamma_2(0)) \leq k$ and $d(\gamma_1(T_1), \gamma_2(T_2)) \leq k$. Then for any $t \leq max\{T_1, T_2\}$ the points $\gamma_1(t)$ and $\gamma_2(t)$ are $(4\delta + 3k)$-close.

Proof. Let $T = max\{T_1, T_2\}$, and extend the shorter geodesic to $[0, T]$ by using the constant map. Since geodesic quadrilaterals are 2δ-thin in δ-hyperbolic geodesic metric spaces, there are two cases to consider.

Suppose that $\gamma_1(t)$ is 2δ-close to a point $\gamma_2(t')$ of γ_2. Then $|t - t'| \leq 2\delta + k$ by the

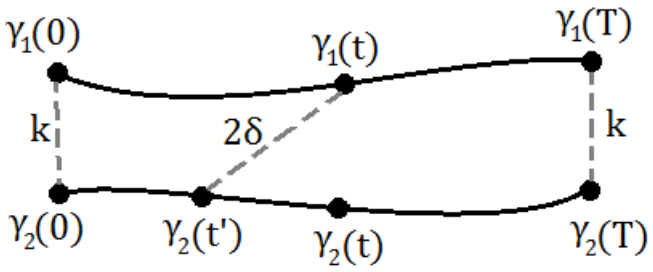

Figure 2.2: Fellow Traveller Property: Case 1

triangle inequality. Thus

$$\begin{aligned} d(\gamma_1(t), \gamma_2(t)) &\leq |t - t'| + 2\delta \\ &\leq 4\delta + k, \end{aligned} \tag{2.18}$$

again by the triangle inequality.

Now suppose that $\gamma_1(t)$ is 2δ-close to a geodesic γ_3 joining $\gamma_1(0)$ to $\gamma_2(0)$. The case for $\gamma_1(t)$ being 2δ-close to the remaining geodesic in this quadrilateral is analogous. It is easy to see that

$$d(\gamma_1(t), \gamma_2(0)) \leq 2\delta + k, \tag{2.19}$$

so by the triangle inequality,

$$t \leq k + (2\delta + k) = 2(\delta + k). \tag{2.20}$$

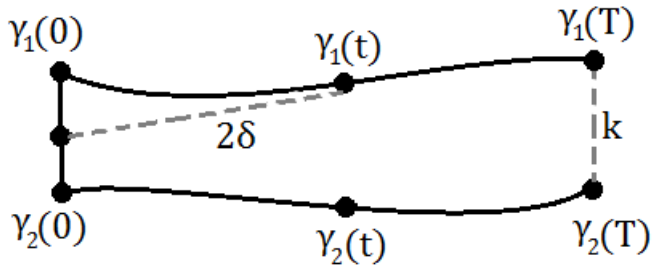

Figure 2.3: Fellow Traveller Property: Case 2

Then combining equations (2.19) and (2.20) we conclude that

$$\begin{aligned} d(\gamma_1(t), \gamma_2(t)) &\leq d(\gamma_1(t), \gamma_2(0)) + t \\ &\leq 4\delta + 3k. \end{aligned} \tag{2.21}$$

□

2.3 Three classes of groups

In this section, we introduce relatively hyperbolic groups, limit groups and residually free groups, and explain how these classes are related. Full explanations of each class of group, including examples, are given at the beginning of each relevant chapter.

There are several definitions of relatively hyperbolic groups, as explained in Chapter 3. However, we follow the definition provided by Farb, as it explains how relative hyperbolicity is a property of the Cayley graph of the group. We begin with the *coned-off Cayley graph* of a group G:

Definition 2.3.1. Let G be a group with generating set X and let $\mathcal{H} = \{H_i\}_{i \in I}$ be a finite set of finitely generated subgroups in G (called *peripheral subgroups*). If we equip the Cayley graph $\widehat{\Gamma} := \Gamma(G, X \cup \mathcal{H})$ with the usual word metric, then any two elements in the same left coset of a peripheral subgroup $H_i \in \mathcal{H}$ are distance 1 apart. The graph $\widehat{\Gamma}$ is called the *coned-off Cayley graph* of G with respect to $\{H_i\}_{i \in I}$.

Farb [24] suggests an alternative approach to the one above, by taking the Cayley graph $\Gamma = \Gamma(G, X)$ and adding a new vertex $v(gH_i)$ for each left coset gH_i, then adding an edge $e(gh)$ of length $\frac{1}{2}$ from each element gh of the coset to this new vertex. The resultant graph is quasi-isometric to the graph $\widehat{\Gamma}$.

Definition 2.3.2. A finitely generated group G is called *weakly relatively hyperbolic* with respect to the subgroups $\mathcal{H}$ if the coned-off Cayley graph of G with respect to $\mathcal{H}$ is hyperbolic with respect to the word metric.

In order for a group to be a relatively hyperbolic group, it must be weakly relatively hyperbolic, and it must satisfy one further property, called the Bounded Coset Penetration property (Definition 3.1.19). The definition of this property contains a lot of technical vocabulary which is explained in detail in Chapter 3. The important point for the reader at this stage is to see relatively hyperbolic groups as a subclass of the class of weakly relatively hyperbolic groups, with extra restrictions on the Cayley graph.

The second class of groups in this thesis is limit groups, which we now define.

Definition 2.3.3. A group G is said to be *fully residually free* if for any finite subset U of G there is a homomorphism ψ from G to a free group F such that the restriction of ψ to U is injective.

Although limit groups were introduced by Sela as the limits of stable sequences of homomorphisms, the definition used in this thesis is Theorem 4.6 from the same paper [49].

Definition 2.3.4. A *limit group* is a finitely generated fully resudually free group.

The first connection between the three classes of groups introduced in this section is that limit groups are hyperbolic relative to their maximal non-cyclic abelian subgroups [20]. Since the conjugacy search problem is trivial in abelian groups, the result for the conjugacy search problem in relatively hyperbolic groups will provide us with a length bound for the conjugacy search problem in limit groups. However, in Chapter 4 we improve this bound significantly, using properties particular to limit groups. We then extend this result to the multiple conjugacy search problem, using the fact that limit groups are *commutative-transitive*. The significance of this property will be explained fully in Chapter 4.

Definition 2.3.5. A group G is said to be *commutative-transitive* if the commutativity property is a transitive relation. That is to say, for any $a, b, c \in G$ such that $aba^{-1}b^{-1} = 1$ and $bcb^{-1}c^{-1} = 1$ then $aca^{-1}c^{-1} = 1$.

The third class of groups is finitely generated residually free groups.

Definition 2.3.6. A group G is *residually free* if for any nonidentity element $g \in G$ there is a homomorphism ϕ into a free group such that $\phi(g) \neq 1$.

Every fully residually free group is clearly residually free. Hence limit groups are a subclass of residually free groups, but there is another link between these limit groups and residually free groups.

Definition 2.3.7. Let $G_1, \ldots, G_n$ be a set of groups. A group

$$S < G_1 \times \cdots \times G_n \tag{2.22}$$

is a *subdirect product* of $G_1, \ldots, G_n$ if each projection

$$p_i : S \to G_i \tag{2.23}$$

is surjective. The group S is a *full* subdirect product if it intersects each of the direct factors G_i nontrivially.

Every finitely presentable residually free group is a full subdirect product of finitely many limit groups [32]:

$$G \leq D := L_1 \times \cdots \times L_n. \tag{2.24}$$

2.4 Subgroup distortion

Definition 2.4.1. Let $G = \langle Y \mid R \rangle$ be a finitely generated group, and let $H = \langle Z \mid S \rangle$ be a finitely generated subgroup of G. Define the function $\Delta_H^G : \mathbb{N} \to \mathbb{N}$ by

$$\Delta_H^G : \ell \mapsto \max\{\|h\|_Z : h \in H, \|h\|_Y \leq \ell\}. \tag{2.25}$$

If this function is linear in ℓ then H is said to be *undistorted* in G. Otherwise H is *distorted* in G.

Definition 2.4.2. Let Δ_1, Δ_2 be two different distortion functions. We say that Δ_1 is *asymptotically less than* Δ_2, written $\Delta_1 \preccurlyeq \Delta_2$, if there is $N \in \mathbb{N}$ such that $\Delta_1(\ell) \leq N\Delta_2(N\ell)$. If $\Delta_1 \preccurlyeq \Delta_2$ and $\Delta_2 \preccurlyeq \Delta_1$ then we say that Δ_1 is *asymptotically equivalent* to Δ_2, written $\Delta_1 \approx \Delta_2$.

Provided that G and H are finitely generated, the distortion functions with respect to different choices Y', Z' of generating sets are asymptotically equivalent. Hence we can talk about *the* distortion function of a subgroup inside a group, with the implicit assumption that the distortion functions are asymptotically equivalent.

Suppose $K \leq H \leq G$ is a chain of subgroups, then $\Delta_K^G(\ell) \leq \Delta_K^H(\Delta_H^G(\ell))$.

The following example shows that there are groups for which distortion in particular subgroups is not linear.

Example 2.4.3. Let $G = \langle a, b \mid b^{-1}ab = a^2 \rangle$. The subgroup $H = \langle a \rangle$ has at least exponential distortion in G.

Proof. Consider the element a^{2^n}. In H, $\|a^{2^n}\|_H = 2^n$. However, in G:

$$\begin{aligned} a^{2^n} &= (a^2)^{2^{n-1}} = (b^{-1}ab)^{2^{n-1}} = ((b^{-1}ab)^2)^{2^{n-2}} \\ &= (b^{-1}a^2b)^{2^{n-2}} = (b^{-2}ab^2)^{2^{n-2}} = \ldots = b^{-n}ab^n \end{aligned} \tag{2.26}$$

and so $\|a^{2^n}\|_G = \|b^{-n}ab^n\|_G = 2n+1$. Hence there is an element which is exponentially distorted in the subgroup H. □

Definition 2.4.4. A *retract* of a group G is a subgroup H for which there is an endomorphism of G which maps surjectively onto H, and is the identity when restricted to H.

Definition 2.4.5. Let $\mathcal{P}$ be a group property. We say that a group G is *virtually* $\mathcal{P}$ if G contains a finite index subgroup which has property $\mathcal{P}$.

Example 2.4.6. Suppose that G is a *virtually nilpotent* group. Then G contains a finite index subgroup which is nilpotent.

Example 2.4.7. Suppose that H is a *virtual retract* of a group G. Then there exists a finite index subgroup K of G such that H is a retract of K.

Lemma 2.4.8. *Finitely generated subgroups are undistorted in limit groups.*

Proof. Let L_1 be a limit group and L_2 a finitely generated subgroup of L_1. By [55, Theorem B], L_2 is a virtual retract of L_1. Finite index subgroups and retracts are undistorted in their ambient groups, and so the result immediately follows. □

Chapter 3

Relatively hyperbolic groups

In this chapter we introduce the class of relatively hyperbolic groups and prove that the asymptotic bound for a length-based attack on the conjugacy search problem in relatively hyperbolic groups is cubic for hyperbolic elements and a "small" polynomial for parabolic elements, which is dependent upon the assumed polynomial bound on the conjugacy search problem for the peripheral subgroups.

The concept of relatively hyperbolic groups was introduced by Gromov [28] as a generalisation of several geometric concepts such as Gromov hyperbolic groups (no peripheral subgroups), geometrically finite Kleinian groups (hyperbolic relative to the maximal parabolic subgroups), and the fundamental groups of finite-volume non-compact Riemannian manifolds of pinched negative sectional curvatures (hyperbolic relative to the fundamental groups of the ends in the manifold). Bowditch [10] later developed the Gromov approach to relatively hyperbolic groups, characterising relatively hyperbolic groups in terms of the dynamics of properly discontinuous isometric group actions on hyperbolic spaces.

An alternative definition was proposed by Farb [24], who characterised (weakly) relatively hyperbolic groups using the coned-off Cayley graph definition (see Definition 2.3.2), and introduced the bounded coset penetration property (see Definition 3.1.19). Farb's definition, without the bounded coset penetration property requirement, is a weaker condition than that of Gromov (as proved by Szczepański, [53]) and hence is referred to in subsequent literature as "Farb's definition" or "weakly relatively hyperbolic groups". However, Dahmani and Bumagin showed that Farb's definition, coupled with the requirement that these groups satisfy the bounded coset penetration property, is equivalent to that of Gromov (see [20],[17] respectively). Such groups are also called "strongly relatively hyperbolic groups" when referring to Farb's definition.

In his paper, Farb proved some useful properties about strongly relatively hyperbolic groups. For example, if the peripheral subgroups have a word problem solvable in $\mathcal{O}(f(n))$-time, then the word problem is solvable in $\mathcal{O}(f(n)\log n)$-time in the ambient strongly relatively hyperbolic group. Furthermore, any isoperimetric function

for the peripheral subgroups is an isoperimetric function for the ambient strongly relatively hyperbolic group. Farb also gave some solutions to the word problem for particular types of groups, namely: an $\mathcal{O}(n \log n)$-time solution for the fundamental group of a finite-volume non-compact Riemannian manifold of pinched negative sectional curvatures, and for hyperbolic knot and link complements.

A further definition of relatively hyperbolic groups, in terms of isoperimetric inequalities, was developed by Osin [46], who then used van Kampen diagrams to establish some algebraic and algorithmic properties of relatively hyperbolic groups. This approach eliminates the need to assume that the relatively hyperbolic group and its peripheral subgroups are finitely generated (and that there are finitely many peripheral subgroups) which allows one to use cancellation over free products - for example, in a separate paper [45], Osin used small cancellation to construct the first examples of finitely generated groups other than $\mathbb{Z}/2\mathbb{Z}$ with precisely two conjugacy classes. Much of the notation and vocabulary in this section is borrowed from Osin's book [46], although we use the Farb definition of strongly relatively hyperbolic groups.

3.1 Preliminaries

Recall the definition of the coned-off Cayley graph (Definition 2.3.1). For a path p in the Cayley graph $\Gamma := \Gamma(G, X)$ we denote the corresponding path in the coned-off graph $\widehat{\Gamma}$ as $\hat{p}$. The path metrics in Γ and $\widehat{\Gamma}$ will be denoted by d_Γ and $d_{\widehat{\Gamma}}$ respectively. To be clear on the choice of generating set, the length of an element x of G with respect to the generating set X will be denoted $\|x\|_X$ and the relative length of x with respect to $X \cup \mathcal{H}$ will be denoted $\|x\|_{X\cup\mathcal{H}}$. The length of a path p in Γ will be denoted $l_\Gamma(p)$ and the length of a path $\hat{p}$ in $\widehat{\Gamma}$ will be denoted $l_{\widehat{\Gamma}}(\hat{p})$.

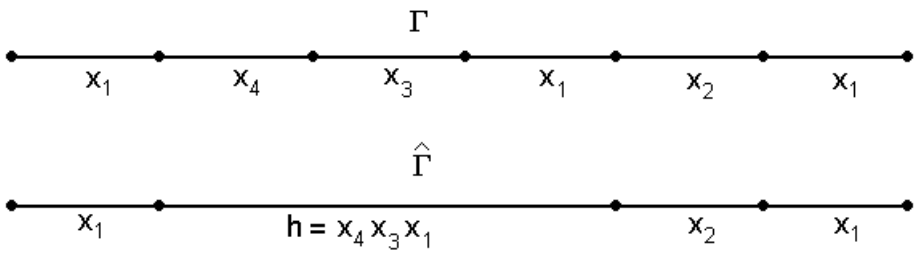

Figure 3.1: An example of the relative length of a path

Figure 3.1 is an example of the relative length of a path. Let $x_i \in X$ for $1 \leq i \leq 4$ and let $x_4x_3x_1$ be an element of a peripheral subgroup. Then $l_\Gamma(p) = 6$ and $l_{\widehat{\Gamma}}(\hat{p}) = 4$.

Definition 3.1.1. A shortest path between two vertices in the Cayley graph is called a *geodesic*. In the coned-off graph a shortest path between two vertices is called a *relative geodesic*.

Definition 3.1.2. A path p between two vertices v_1, v_2 in the Cayley graph is called a (λ, c)-*quasigeodesic* (or just a *quasigeodesic*) if for all subpaths s of p,

$$\frac{1}{\lambda} l_\Gamma(s) - c \leq l_{\widehat{\Gamma}}(\hat{s}) \leq \lambda l_\Gamma(s) + c. \tag{3.1}$$

In the coned-off graph, a quasigeodesic is called a *relative quasigeodesic*.

The label of a path p in a Cayley graph will be written in this chapter as $\phi(p)$ and will be identified with the element it represents in G. The centraliser of an element $g \in G$ will be written as $C_G(g)$.

We denote the origin and terminus of a path p by p_- and p_+ respectively.

Definition 3.1.3. Two paths p, q in a graph are called k-*similar* if

$$d_\Gamma(p_-, q_-) \leq k \text{ and } d_\Gamma(p_+, q_+) \leq k. \tag{3.2}$$

Definition 3.1.4. We say that two paths p, q are *symmetric* if $\phi(p) \equiv \phi(q)$, i.e. if the two paths have identical labels.

Definition 3.1.5. Given a pair of symmetric paths (p, q) we call $g_1 = (p_-)^{-1} q_-$ and $g_2 = (p_+)^{-1} q_+$ the *characteristic elements* of (p, q).

Definition 3.1.6. A symmetric pair of geodesics (p, q) is said to be *minimal* if for any other pair of symmetric geodesics (p', q') with the same characteristic elements, the inequality $l_{\widehat{\Gamma}}(\hat{p}) \leq l_{\widehat{\Gamma}}(\hat{p'})$ holds.

Definition 3.1.7. Let (p, q) be a symmetric pair of paths. We say that the vertices v_1 of p and v_2 of q are *synchronous vertices* if the path segments $[p_-, v_1]$ and $[q_-, v_2]$ have the same length.

Definition 3.1.8. Let H_i be a peripheral subgroup of a relatively hyperbolic group G. A subpath is called an H_i-*component* if it is labelled by an element of H_i, and it is maximal in that respect (it is not contained in a larger subpath which is labelled by an element in H_i).

Definition 3.1.9. A path p in Γ is said to *penetrate* a coset fH_i if p contains an H_i-component s with initial vertex s_- which is labelled by an element of fH_i. This vertex is the point at which p penetrates the coset.

Definition 3.1.10. Any vertex of a path p which "disappears" in the coned-off graph $\widehat{\Gamma}$ (that is, any vertex which is part of some H_i-component s but is not equal to s_- or s_+) is called *non-phase*. All other vertices are called *phase* vertices.

Example 3.1.11. Consider the two paths in Figure 3.1. The two vertices which are present in Γ (top) but not in $\widehat{\Gamma}$ (bottom) are non-phase vertices. The other fiver vertices are phase vertices.

Definition 3.1.12. Two H_i-components s of p and t of q are called *synchronous* components if s_- and t_- are synchronous vertices. Otherwise we can say that s and t are *asynchronous*.

Definition 3.1.13. Two H_i-components s of p and t of q are *connected* components if there is a path in Γ from s_- to t_- which is labelled by an element of H_i.

Remark 3.1.14. Two H_i-components s, t which penetrate the same coset are connected components, since there is an edge in the Cayley graph Γ which joins s_- to t_- and is labelled by an element of H_i.

We state without proof a useful lemma from [46]:

Lemma 3.1.15. *Let $(\hat{p}, \hat{q})$ be a minimal pair of symmetric geodesics in the Cayley graph $\Gamma(G, X \cup \mathcal{H})$.*

1. *Suppose that, for some i, two H_i-components a and b of $\hat{p}$ and $\hat{q}$ respectively are connected. Then a and b are synchronous.*

2. *Let u_1, v_1 and u_2, v_2 be two pairs of synchronous vertices of $\hat{p}$ and $\hat{q}$ respectively. Then $(u_1)^{-1}v_1 \neq (u_2)^{-1}v_2$.*

Remark 3.1.16. In Bumagin's paper on the conjugacy problem in relatively hyperbolic groups [16] there is a case in which a minimal pair of symmetric geodesics p, q penetrate a coset fH_i asynchronously - that is to say, the vertices at which p and q penetrate fH_i are asynchronous. This is Lemma 5.5 ("skew" cosets) and Section 5.1 (Cascades) of [16].

However, by Remark 3.1.14, if p and q both penetrate a coset fH_i then this is equivalent to saying that p and q contain connected H_i-components. By Lemma 3.1.15, since these components are connected then they are synchronous.

Hence the cases of "skew" cosets and "cascades" cannot occur, which simplifies Bumagin's argument.

Definition 3.1.17. When we speak of a single path p in Γ, we say that an H_i-component s is *isolated* if no distinct H_i-component of p is connected to s by a path in Γ labelled by an element of H_i.

Definition 3.1.18. A path p is called a *path without backtracking* if every H_i-component of p is isolated.

Recall that a finitely generated group G is called *weakly relatively hyperbolic* with respect to the subgroups $\mathcal{H}$ if the coned-off Cayley graph of G with respect to $\mathcal{H}$ is hyperbolic with respect to the word metric. (Definition 2.3.2)

A further property is required for such a group to be called relatively hyperbolic:

Definition 3.1.19. Bounded Coset Penetration Property. Let G be a weakly hyperbolic group relative to the subgroups $\{H_i\}_{i\in I}$. Then G is said to *satisfy the Bounded Coset Penetration property (BCP)* if for any λ there exists a constant $c(\lambda)$ such that the following conditions hold. Let p, q be two paths which are relative $(\lambda, 0)$-quasi-geodesics without backtracking, with the same endpoints.

1. If both p and q penetrate the same left coset then they enter (and leave) the coset a distance at most $c(\lambda)$ apart.

2. If p penetrates a left coset gH_i which q does not penetrate, then p travels a distance at most $c(\lambda)$ in gH_i.

Figure 3.2 represents an illustration of the Bounded Coset Penetration property. This is a subgraph of the Cayley graph of a relatively hyperbolic group. This subgraph is two relative $(\lambda, 0)$-quasi-geodesics without backtracking, with the same endpoints. The grey areas represent vertices in the graph Γ which belong to two left cosets, g_1H_1 and g_2H_2. Here $d_\Gamma(u_i, v_i) \leq c(\lambda)$ for $i = 1, 2$ and $d_\Gamma(v_3, v_4) \leq c(\lambda)$.

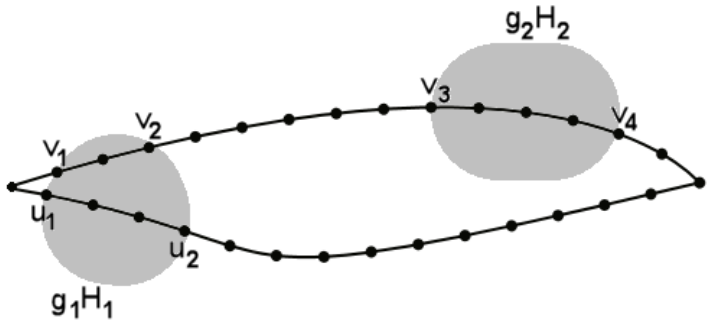

Figure 3.2: Bounded Coset Penetration

Definition 3.1.20. A finitely generated group G is said to be *hyperbolic relative to its subgroups* $\mathcal{H}$ (or simply *relatively hyperbolic*) if it is weakly relatively hyperbolic with respect to $\mathcal{H}$ and it satisfies the Bounded Coset Penetration property.

We illustrate the bounded coset penetration property of relatively hyperbolic groups by providing two examples. The group in Example 3.1.21 is weakly relatively hyperbolic, but does not satisfy the bounded coset penetration property. The

group in Example 3.1.22 is strongly relatively hyperbolic, that is to say: it is weakly relatively hyperbolic and it satisfies the bounded coset penetration property.

Example 3.1.21. Let $G = A \times F$ where $A = \langle a, b \mid ba = ab \rangle$ (the free abelian group generated by a, b) and $F = \langle c \rangle$ (the free group generated by c), and choose the peripheral subgroup to be $H = \{(x, 1) \mid x \in A\}$. Then G is weakly relatively hyperbolic with respect to H, but it is not (strongly) relatively hyperbolic with respect to H.

Proof. The first thing to note is that left cosets of H are of the form (A, c^i) where $i \in \mathbb{Z}$. The coned-off Cayley graph $\widehat{\Gamma} = \Gamma(G, \{a, b, c\} \cup H)$ is quasi-isometric to a bi-infinite path, which is clearly hyperbolic as a metric space. It follows that $\widehat{\Gamma}$ is also a hyperbolic metric space, so G is weakly relatively hyperbolic. However, for any $n \in \mathbb{N}$, the path

$$p_1 = (xa^{-1}, c^i), (xa^n, c^i), (xa^n, c^{i+1}), \ldots, (xa^n, c^j), (y, c^j) \tag{3.3}$$

is a quasi-geodesic with the same endpoints as the quasi-geodesic path

$$p_2 = (xa^{-1}, c^i), (x, c^i), (x, c^{i+1}), \ldots, (x, c^j), (y, c^j) \tag{3.4}$$

and these two paths both penetrate the left coset (A, c^i), but they leave this coset a Γ-distance n apart. Since we can choose arbitrarily large n, this violates the BCP property. □

Example 3.1.22. Let G be the free product of two finitely generated groups $H = \langle X|R \rangle$ and $N = \langle Y|S \rangle$, such that H is a hyperbolic group. Then G is hyperbolic relative to N.

Proof. We can say that G is generated by $X \cup Y$. Elements of G can be expressed in the reduced form

$$g = \alpha_1 \beta_1 \alpha_2 \beta_2 \ldots \alpha_n \beta_n, \tag{3.5}$$

where $\alpha_i \in H \backslash \{1\}$ is reduced according to the relations of H and $\beta_i \in N \backslash \{1\}$ is reduced according to the relations of N for all $i = 1, \ldots, n$, and α_1 & β_n can also be equal to the identity element. The reduced form as shown above is not unique to each element, since the relations in H and N may allow us to write each nontrivial syllable of g in several ways, but the length n is unique to each word in G. First we look at what equality of two words over the alphabet $X \cup N$ signifies in terms of the coned-off Cayley graph $\widehat{\Gamma} = \Gamma(G, X \cup N)$. For $i = 1, 2$ let p_i be two geodesic paths with same endpoints in $\widehat{\Gamma}$, with labels

$$\phi(p_i) = \alpha_1^{(i)} \beta_1^{(i)} \alpha_2^{(i)} \beta_2^{(i)} \ldots \alpha_n^{(i)} \beta_n^{(i)} \tag{3.6}$$

in reduced form, and assume that these two labels represent the same element in G.

The N-syllables (that is, the β-terms) each label a single edge of the corresponding path p_i (since p_i are geodesics in $\widehat{\Gamma}$), so where there is algebraic equality, the corresponding edges are also equal. The H-syllables (i.e., the α-terms) are elements of the subgroup H, so they label subpaths of each p_i. However, by the δ-hyperbolicity of H, a simple "thin triangles" argument (forming a triangle by splitting one of these subpaths in two pieces) reveals that where there is algebraic equality, the corresponding subpaths are δ-close.

Let T be a geodesic triangle in $\widehat{\Gamma}$ with sides (as read clockwise) s_1, s_2, s_3, where

$$\phi(s_i) = \alpha_1^{(i)}\beta_1^{(i)}\alpha_2^{(i)}\beta_2^{(i)}\dots\alpha_{k_i}^{(i)}\beta_{k_i}^{(i)}. \tag{3.7}$$

Since this triangle is a loop in Γ, we see that $\phi(s_1^{-1}) = \phi(s_2)\phi(s_3)$. That is,

$$\begin{aligned}(\alpha_1^{(1)}\beta_1^{(1)}\dots\alpha_{k_1}^{(1)}\beta_{k_1}^{(1)})^{-1} &= (\beta_{k_1}^{(1)})^{-1}(\alpha_{k_1}^{(1)})^{-1}\dots(\beta_1^{(1)})^{-1}(\alpha_1^{(1)})^{-1} \\ &= (\alpha_1^{(2)}\beta_1^{(2)}\dots\alpha_{k_2}^{(2)}\beta_{k_2}^{(2)})(\alpha_1^{(3)}\beta_1^{(3)}\dots\alpha_{k_3}^{(3)}\beta_{k_3}^{(3)})\end{aligned} \tag{3.8}$$

Note that either $\beta_{k_1}^{(1)} = 1$ or $\alpha_1^{(2)} = 1$. Likewise $\alpha_1^{(1)} = 1$ or $\beta_{k_3}^{(3)} = 1$. If the number of nontrivial components on either side of the equation is equal, then s_2s_3 is a geodesic path in $\widehat{\Gamma}$ with the same endpoints as s_1. By the above argument these two geodesics are δ-close, so our triangle T is δ-thin.

We assume the alternative. Then there is cancellation where the two words meet, until the bottom line of equation (3.8) has length k_1. Either $\beta_{k_2}^{(2)}$ or $\alpha_1^{(3)}$ is equal to the identity. Let us assume that $\beta_{k_2}^{(2)} = 1$ (the argument for $\alpha_1^{(3)} = 1$ is analogous). This cancellation corresponds geometrically to backtracking of the path s_2s_3. If we say that the first (respectively, last) k nonidentity syllables of $\phi(s_3)$ (respectively, $\phi(s_2)$) are involved in the cancellation, these syllables correspond to two subgeodesics of s_3 and s_2 respectively with same endpoints. These subgeodesics are δ-close by the above argument. The remainder of the geodesics s_3 and s_2 join to form a geodesic γ of length k_3 with same endpoints as s_1. The geodesics γ and s_1 are (as argued above) δ-close to each other. Then T is a δ-thin triangle, so $\Gamma(G, X \cup N)$ is δ-hyperbolic as a metric space. Therefore G is a weakly relatively hyperbolic group.

To prove strong relative hyperbolicity we consider two $(\lambda, 0)$-quasi-geodesics p, q without backtracking, with same endpoints, in $\Gamma(G, X \cup N)$. Since p and q have the same endpoints their labels have the same reduced form under the group relations, however we cannot immediately assume that the labels of p and q are in reduced form. The only relations are R of the group H and N of the group S. In particular, there are no relations involving elements from both H and N. Furthermore, by assumption p and q do not backtrack, so there are no subwords of the labels $\phi(p), \phi(q)$ which read

"$\alpha_i\alpha_i^{-1}$" or "$\beta_i\beta_i^{-1}$" for some i. Hence $\phi(p)$ and $\phi(q)$ are both in semi-reduced form:

$$\phi(p) = \alpha_1^{(p)}\beta_1^{(p)}\dots\alpha_n^{(p)}\beta_n^{(p)} \text{ and } \phi(q) = \alpha_1^{(q)}\beta_1^{(q)}\dots\alpha_n^{(q)}\beta_n^{(q)} \tag{3.9}$$

where, for each i, $\alpha_i^{(p)} = \alpha_i^{(q)}$ under the relations of H and $\beta_i^{(p)} = \beta_i^{(q)}$ under the relations of N, but the α_i and β_i terms are not necessarily reduced according to the relations in H and N respectively. This is what distinguishes them from geodesics with the same endpoints.

Cosets of G are of the form $\alpha_1\beta_1\dots\alpha_kN$. Edges entering or leaving a left coset are labelled by elements of the generating set X of H. Therefore any edge entering a left coset $\alpha_1\beta_1\dots\alpha_kN$ must terminate at a vertex whose label ends in some element of H. The only such vertex in this coset is $\alpha_1\beta_1\dots\alpha_k$. Likewise in order for a path to leave a coset $gN = \alpha_1\beta_1\dots\alpha_kN$ and enter another coset with the prefix $\alpha_1\beta_1\dots\alpha_k\beta_k$, it must leave gN at the vertex $\alpha_1\beta_1\dots\alpha_k\beta_k$. Thus p and q both visit the vertices $\alpha_1\beta_1\dots\alpha_i$ and $\alpha_1\beta_1\dots\alpha_i\beta_i$ for each $i \in \{1,\dots,n\}$.

Between $\alpha_1\beta_1\dots\alpha_k$ and $\alpha_1\beta_1\dots\alpha_k\beta_k$ both quasi-geodesics are travelling inside the left coset $\alpha_1\beta_1\dots\alpha_kN$, which they enter and exit at the same vertex. Between $\alpha_1\beta_1\dots\alpha_k\beta_k$ and $\alpha_1\beta_1\dots\alpha_k\beta_k\alpha_{k+1}$ they may not visit the same cosets, but they only visit one vertex in each coset. It follows that the bounded coset penetration property is satisfied, so G is a relatively hyperbolic group. □

The following proposition is essentially a rewording of the bounded coset penetration property, except with k-similar quasi-geodesics instead of quasi-geodesics with same endpoints. This is taken directly from Osin's book [46].

Proposition 3.1.23. *There is a polynomial $\varepsilon = \varepsilon(\lambda, c, k)$ such that for any two k-similar (λ, c)-quasi-geodesics without backtracking p, q in $\Gamma(G, X \cup \mathcal{H})$, the following conditions hold:*

1. *The sets of phase vertices of p and q are contained in the closed ε-neighbourhoods of each other.*
2. *Suppose that s is an H_i-component of p such that $d_X(s_-, s_+) > \varepsilon$, then there exists an H_i-component t of q which is connected to s.*
3. *Suppose that s and t are connected H_i-components of p and q respectively. Then $max\{d_\Gamma(s_-, t_-), d_\Gamma(s_+, t_+)\} \leq \varepsilon$.*

The existence of ε is due to Theorem 3.23 of [46]. Details of the proof can be found in that book. The fact that ε is a polynomial was shown by [30].

Proposition 3.1.24. *The polynomial ε is a quadratic function of k.*

Proof. To write an explicit formula for ε we need a few other formulae. Firstly, it is shown in [11] that two k-similar (λ, c)-quasi-geodesics in a δ-hyperbolic metric space are contained in the K-neighbourhood of each other. In [30] it is shown that we can use the function

$$K = (\delta \log_2(2\lambda^3 + 6\lambda^2 + 3\lambda + 2) + \delta \log_2(\delta \log_2(2\lambda^3 + 6\lambda^2 + 3\lambda + 2)) + 1)(\lambda^2 + 1)$$
$$+\frac{1}{2}(2\lambda^3 + 3\lambda) + k + 2\delta, \tag{3.10}$$

which is a linear function of k and is bounded by a polynomial in λ.

Secondly, for any two k-similar (λ, c)-quasi-geodesic paths without backtracking p, q in $\Gamma(G, X \cup \mathcal{H})$, [46] has shown that the set of phase vertices of p is contained within the A-neighbourhood of the set of phase vertices of q, and vice versa, where

$$A = KLM(8\lambda K + 2K + 2c) \tag{3.11}$$

with K as above, and $LM > 1$ is a constant (see [46], Convention 3.1 for details).

Now, we can write the polynomial as

$$\varepsilon = LM(2 + 2\lambda(A + 1) + c + 2A). \tag{3.12}$$

This is a λ-polynomial of degree at most 8, and a k-quadratic.

It is important to note that if p and q are geodesics then $\lambda = 1$ and $c = 0$, so $A \leq 10K^2LM$, and we can use $\varepsilon(1, 0, k) \leq 4LM(1 + 10(K')^2LM)$ which is simply a quadratic function of k. □

3.2 Conjugacy search problem

The aim of this section is to find an upper bound U for the minimum length of a conjugating element, so that the conjugacy search problem can be solved by checking with all elements x of length less than U whether $x^{-1}axb^{-1} = 1$ in G. The word problem in relatively hyperbolic groups was shown by Farb to have a solution bounded as follows:

Theorem 3.2.1 ([24])**.** *Suppose that a group G is hyperbolic relative to a subgroup H, and H has word problem solvable in time $O(f(n))$. Then there is an algorithm which gives an $O(f(n) \log n)$-time solution to the word problem in G.*

In [16] Bumagin proved that the conjugacy problem is solvable for relatively hyperbolic groups. Ji, Ogle and Ramsey used this paper to show that the conjugacy search problem for relatively hyperbolic groups has a polynomial conjugacy length bound, provided the conjugacy length bound for the peripheral subgroups is at worst

polynomial [30]. Let n be the degree of the polynomial bound for the conjugacy search problem in the peripheral subgroups. A detailed study of [30] shows that this bound is a polynomial of degree $576n$ (Using the calculation (3.12) of ε as a λ-polynomial of degree at most 8). The results in this section drastically improve this estimate, with a much shorter proof.

Throughout this section G will denote a group which is relatively hyperbolic with respect to the peripheral subgroups $\mathcal{H} = \{H_i\}_{i\in I}$, with finite generating set X. Given two conjugate elements $a, b \in G$, our goal is to find an element x which satisfies the equation $x^{-1}axb^{-1} = 1$. Geometrically, we want to find a closed path $\Theta := \theta_q^{-1}\theta_a\theta_p\theta_b^{-1}$ in the Cayley graph of G such that $\phi(\theta_a) = a$, $\phi(\theta_b) = b$ and $\phi(\theta_p) = \phi(\theta_q) = x$ - see Figure 3.3. We may assume that the path θ_a starts at the vertex labelled by the identity element. The subpaths θ_p and θ_q are symmetric and $\mathcal{L}$-similar, where

$$\mathcal{L} = \max\{\|a\|_X, \|b\|_X\}. \tag{3.13}$$

We want to find an upper bound on the length of the element x, so we will assume that (θ_p, θ_q) is a minimal pair of symmetric geodesics, and we attempt to establish an upper bound on the Γ-length of these geodesics.

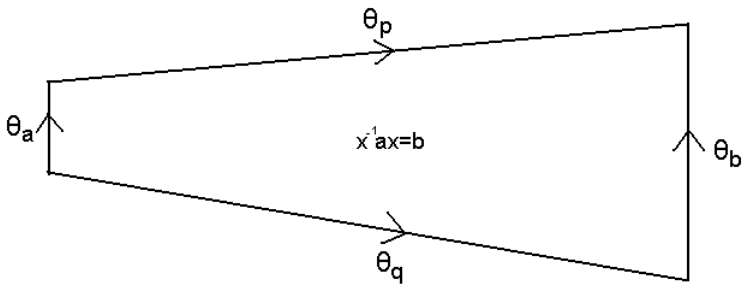

Figure 3.3: Conjugacy diagram showing Θ in $\Gamma(G, X)$

Definition 3.2.2. An element g of the relatively hyperbolic group G is *parabolic* if it is conjugate to some element of one of the peripheral subgroups $\mathcal{H}$, otherwise it is called *hyperbolic*.

Lemma 3.2.3. *Let $a \in G$ be conjugate to an element b, and let x be a conjugating element of minimal length. Consider the coned-off Cayley graph $\widehat{\Gamma}$. If (u, v) is a pair of synchronous vertices on $(\hat{\theta}_p, \hat{\theta}_q)$ with $d_{\widehat{\Gamma}}((\hat{\theta}_p)_\pm, u) > \mathcal{L} + 2\delta$, then $d_{\widehat{\Gamma}}(u, v) \leq 4\delta$.*

Proof. As usual we assume that $\hat{\theta}_p$ and $\hat{\theta}_q$ are chosen to be minimal. We parametrize $\hat{\theta}_p$ and $\hat{\theta}_q$ so that $\hat{\theta}_p(i)$ is the i^{th} vertex along the path $\hat{\theta}_p$, and likewise with $\hat{\theta}_q$. Let

$u = \hat{\theta}_p(t)$, then $v = \hat{\theta}_q(t)$.

By the 2δ-thinness of quadrilaterals in hyperbolic spaces, there is some vertex $\hat{\theta}_p(t')$ which is 2δ-close to $\hat{\theta}_q(t)$. Suppose without loss of generality that $t' \geq t$. Then $\hat{\theta}_p(t)$ is 2δ-close to $\hat{\theta}_r(t')$, where $\hat{\theta}_r = a\hat{\theta}_p$ (see Figure 3.4).

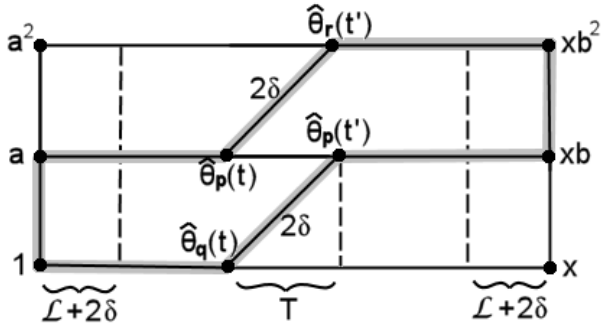

Figure 3.4: Conjugacy diagram for Lemma 3.2.3

If $T = t' - t > 2\delta$ then the paths

$$[a, \hat{\theta}_p(t)][\hat{\theta}_p(t), \hat{\theta}_r(t')][\hat{\theta}_r(t'), xb^2] \tag{3.14}$$

and

$$[1, \hat{\theta}_q(t)][\hat{\theta}_q(t), \hat{\theta}_p(t')][\hat{\theta}_p(t'), xb] \tag{3.15}$$

are shorter than $\hat{\theta}_p$ and $\hat{\theta}_q$, and they conjugate a and b (as highlighted in grey on the diagram), which contradicts our assumption that $(\hat{\theta}_p, \hat{\theta}_q)$ is a minimal pair of synchronous geodesics. It now follows from the triangle inequality that

$$d_{\widehat{\Gamma}}(u, v) \leq T + 2\delta \leq 4\delta. \tag{3.16}$$

□

This shows that there is a "middle" section of $\hat{\theta}_p$ whose $\widehat{\Gamma}$-length is bounded by the number of distinct words in $X \cup \mathcal{H}$ of length 4δ. We make use of the following:

Lemma 3.2.4 ([46], Lemma 3.41)**.** *Let (p, q) be a minimal pair of symmetric geodesics in $\Gamma(G, X)$ such that*

$$\max\{d_{\widehat{\Gamma}}(\hat{p}_-, \hat{q}_-), d_{\widehat{\Gamma}}(\hat{p}_+, \hat{q}_+)\} \leq k \tag{3.17}$$

and let v_1, v_2 be synchronous vertices on p and q respectively such that

$$\min\{d_{\widehat{\Gamma}}(\hat{p}_-, v_1), d_{\widehat{\Gamma}}(\hat{p}_+, v_1)\} \geq 2E, \tag{3.18}$$

where $E = 4\delta + 3k$ is the constant from Lemma 2.2.11. Then

$$d_\Gamma(v_1, v_2) \leq 6MLE^2. \tag{3.19}$$

Setting $k = 4\delta$ from equation 3.16 and combining this with the previous lemmas from section 3.1 we have the following:

Lemma 3.2.5. *Let $a \in G$ be conjugate to an element $b \in G$. Then there exists $x \in G$ such that $a = x^{-1}bx$ and*

$$\|x\|_{X\cup\mathcal{H}} \leq 2(\mathcal{L} + 34\delta) + |X|^{6ML(16\delta)^2}, \tag{3.20}$$

where $\mathcal{L} = \max\{\|a\|_X, \|b\|_X\}$.

Proof. We have established in Lemma 3.2.3 that synchronous vertices which are a $\widehat{\Gamma}$-distance of at least $\mathcal{L}+2\delta$ from either end of $\hat{\theta}_p$ and $\hat{\theta}_q$ respectively are a $\widehat{\Gamma}$-distance of at most 4δ apart from each other. Let us call these middle sections $\hat{\theta}'_p$ and $\hat{\theta}'_q$. Then we can use Lemma 3.2.4 with $k = 4\delta$ to prove that if (u, v) is a pair of synchronous phase vertices on the paths θ_p and θ_q in Γ such that

$$d_{\widehat{\Gamma}}(u, (\theta'_p)_\pm) \geq 2E = 2(4\delta + 3(4\delta)) = 32\delta \tag{3.21}$$

then

$$d_\Gamma(u, v) \leq 6ML(16\delta)^2. \tag{3.22}$$

Thus the length of the section of θ_p in Γ which is a coned-off $\widehat{\Gamma}$-distance of $\mathcal{L} + 34\delta$ from either end of θ_p has Γ-length at most $|X|^{6ML(16\delta)^2}$ by the argument that if there are two pairs of synchronous vertices which are joined by a geodesic of the same label, then we can shorten the closed path Θ, which represents the conjugation, by "cutting out" the section between these two geodesic paths and joining the remaining parts together along these geodesics.

We conclude that $\hat{\theta}_p$ has a $\widehat{\Gamma}$-length of

$$l_{\widehat{\Gamma}}(\hat{\theta}_p) \leq 2(\mathcal{L} + 34\delta) + |X|^{6ML(16\delta)^2}, \tag{3.23}$$

as illustrated in Figure 3.5, in which lengths are $\widehat{\Gamma}$-lengths unless otherwise stated. □

The following is drawn from results in [46]:

Lemma 3.2.6. *Let a, b be conjugate hyperbolic elements of G, with a conjugating element x of minimal length. Then the Γ-distance through which the associated paths θ_p and θ_q of the closed path Θ travel in each H_i-coset is bounded above by the quadratic*

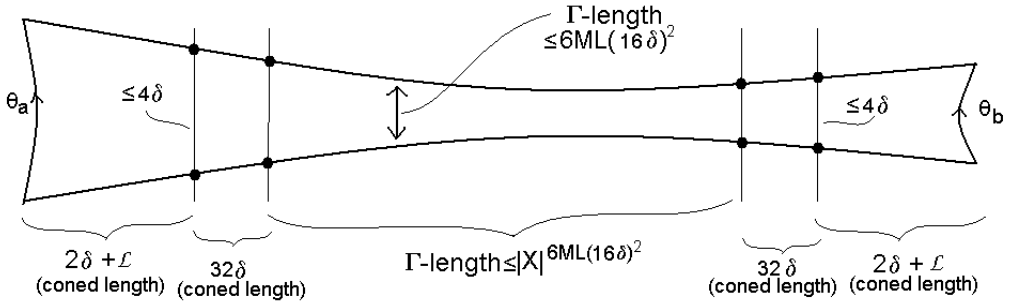

Figure 3.5: Length diagram for Lemma 3.2.5

function $\varepsilon(\mathcal{L})$, where $\mathcal{L} = \max\{\|a\|_X, \|b\|_X\}$, and ε is the quadratic from Proposition 3.1.24.

Proof. Consider the closed cycle Θ in $\Gamma(G, X)$. Proposition 3.1.23 states that if s is an H_i-component of θ_p with $l_\Gamma(s) > \varepsilon$, then there exists an H_i-component t of θ_q which is connected to s by a path labelled by $h \in H_i$. Furthermore, by Lemma 3.1.15, since θ_p and θ_q are minimal and symmetric, and s and t are connected, then these two components are synchronous. Consequently a and b are conjugate to $h \in H_i$, but we are assuming that a and b are hyperbolic, which is a contradiction. Hence $l_\Gamma(s) \leq \varepsilon$. □

Theorem 3.2.7. *Let a and b be conjugate hyperbolic elements of the relatively hyperbolic group G. Then there exists $x \in G$ such that $x^{-1}ax = b$ and $\|x\|_X$ is bounded above by a cubic polynomial in $\mathcal{L} = \max\{\|a\|_X, \|b\|_X\}$.*

Proof. Lemma 3.2.6 shows that θ_p travels a Γ-distance of no more than ε in each coset it penetrates. By Lemma 3.2.5 we know that there is a 'middle section' of θ_p which has Γ-length bounded by the constant $|X|^{6ML(16\delta)^2}$. Either side of this section is a subpath of θ_p which has $\widehat{\Gamma}$-length bounded by $34\delta + \mathcal{L}$. Hence

$$\|x\|_X = l_\Gamma(\theta_p) \leq 2(34\delta + \mathcal{L})\varepsilon + |X|^{6ML(16\delta)^2} \tag{3.24}$$

which is a cubic polynomial in $\mathcal{L}$. □

Lemma 3.2.8. *Let a and b be conjugate parabolic elements in G with respect to $\{H_i\}_{i\in I}$, and suppose that the conjugacy search problem in each of the subgroups H_i is bounded above by a polynomial $\mathcal{P}$ of degree n. Then the paths θ_p and θ_q each travel a polynomially bounded distance, of degree $2n$, in each coset they penetrate.*

Proof. Choose a peripheral subgroup H_i and consider the set $\{(u_j, v_j) : j = 1, \ldots, m\}$ of all synchronous phase vertices on θ_p and θ_q respectively which are each joined by a geodesic path in $\Gamma(G, X \cup \mathcal{H})$ labelled by $h_j \in H_i$, such that θ_p reaches each u_j

in ascending order. Divide the quadrilateral Θ into $m+1$ "cells" using these paths $\{h_j\}_{j=1}^m$. For notational ease, let $h_0 := \theta_a$ and $h_{m+1} := \theta_b$. The segment

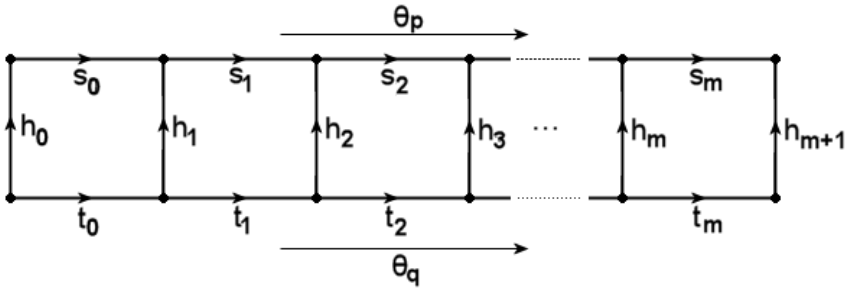

Figure 3.6: Illustration of the "cells" in Lemma 3.2.8

$$s_j := [(h_j)_+, (h_{j+1})_+] \tag{3.25}$$

of θ_p in each cell will fall into one of two categories. In the first case it is an H_i-component, in which case so is

$$t_j := [(h_j)_-, (h_{j+1})_-]. \tag{3.26}$$

Then h_j and h_{j+1} are conjugate in H_i, and the Γ-length of s_j and t_j will be bounded by

$$\mathcal{P}(\max\{l_\Gamma(h_j), l_\Gamma(h_{j+1})\}) \leq \mathcal{P}(\varepsilon), \tag{3.27}$$

where ε is the quadratic from Proposition 3.1.24, so that $\mathcal{P}(\varepsilon)$ is a polynomial of degree $2n$. Note that if s_0 is an H_i-component then $a = h^{-1}h_1h$ for some $h \in H_i$ and hence $a \in H_i$. Likewise if s_m is an H_i-component then $b \in H_i$.

The second case is that s_j is not an H_i-component of θ_p, although it may contain an H_i-component h' of θ_p which, by our choice of the paths h_j, will not be connected to the synchronous H_i-component of θ_q. Since (s_j, t_j) is a minimal pair of synchronous geodesics with characteristic elements h_j and h_{j+1}, we can use Lemma 3.1.15 to see that if h' is connected to any H_i-component of θ_q then these two components must be synchronous. Then by Proposition 3.1.23 and Proposition 3.1.24, as h' is an isolated component, its Γ-length is bounded by ε which is a quadratic function of $\mathcal{L}$.

We conclude that for parabolic a, b the Γ-length of any H_i-component of θ_p is bounded by a polynomial

$$\mathcal{M}(\mathcal{L}) = \max\{\varepsilon, \mathcal{P}(\varepsilon)\}. \tag{3.28}$$

□

Theorem 3.2.9. *Let a and b be conjugate parabolic elements of the relatively hyperbolic group G. Suppose that the conjugacy search problem in each peripheral subgroup can be bounded by a polynomial $\mathcal{P}(\mathcal{L})$ of degree n. Then there exists an element $x \in G$ such that $a^x = b$ and the Γ-length of x is bounded by a polynomial of degree $2n+1$ in $\mathcal{L} = \max\{\|a\|_X, \|b\|_X\}$.*

Proof. As in the hyperbolic case, the Γ-length of θ_p is bounded by

$$2(34\delta + \mathcal{L})\mathcal{M} + |X|^{6ML(16\delta)^2} \tag{3.29}$$

where $\mathcal{M}$ is the polynomial from Lemma 3.2.8. Then $l_\Gamma(\theta_p)$ is bounded above by a polynomial in $\mathcal{L}$ of degree $2n+1$. □

Theorem 3.2.10. *Let G be a relatively hyperbolic group with generating set X, and suppose that the conjugacy search problem in all peripheral subgroups can be bounded by a polynomial $\mathcal{P}$ of degree n. Let $a, b \in G$ be two elements which are conjugate in G, and let $\mathcal{L} = \max\{\|a\|_X, \|b\|_X\}$. Then the conjugacy search problem in G is bounded by a polynomial function of $\mathcal{L}$ of degree* $\max\{3, 2n+1\}$.

Proof. The result follows from Theorem 3.2.7 and Theorem 3.2.9. □

Corollary 3.2.11. *If G is a limit group then for any pair of conjugate elements a, b we can find a conjugating element x of length at most $\mathcal{P}$, where $\mathcal{P}$ is a cubic polynomial in $\mathcal{L} = \max\{\|a\|_X, \|b\|_X\}$.*

Proof. Limit groups are hyperbolic relative to their maximal non-cyclic abelian subgroups [20], and the conjugacy search problem in abelian groups is trivial. Hence $n = 0$ and the cubic bound for the hyperbolic case gives the asymptotic upper bound for $\|x\|_X$. □

The length bound of Theorem 3.2.10 is not optimal in specific cases. For example we can do much better than this for limit groups, as the next chapter shows.

Chapter 4

Limit groups

In this chapter we show that the conjugacy search problem and the multiple conjugacy search problem in limit groups can be solved using elements whose length is a linear function of the input elements.

The *elementary theory* of a group G is the set of first-order sentences in the language of group theory which are true in G. The *existential theory* of a group G is the set of first-order sentences which only use one quantifier, $\exists$, and which are true in G. In 1945 Alfred Tarski asked the following:

1. Do the elementary theories of non-abelian free groups coincide?

2. Is the elementary theory of a non-abelian free group decidable?

The first question was answered in the affirmative by Kharlampovich-Myasnikov ([31], [32]) and Sela (see [49] *et. seq.*) independently. They showed that limit groups are precisely the groups with the same existential theory as a free group. The second question was answered in the affirmative by Kharlampovich-Myasnikov [33].

It was this series of papers in which limit groups were extensively studied, under various definitions which were all shown to be equivalent. It was Sela [49] who coined the term "limit group" to emphasise that these groups are the ones which arise when one takes limits of stable sequences of homomorphisms $\phi_n : G \to F$ from a finitely generated group G to a free group F, but such groups were previously studied under alternative names: as finitely generated, fully residually free groups (In the case of Kharlampovich-Myasnikov) and as finitely generated $\exists$-free groups (groups with the same existential theory as free groups, the study of which was initiated by Remeslennikov [47]).

Remeslennikov [47] showed that a finitely generated group is $\exists$-free if and only if it is fully residually free. Kharlampovich-Myasnikov [34] gave the algebraic description shown in construction 4.2. The equivalence of limit groups with finitely generated, fully residually free groups was demonstrated by Sela [49], a fact which will be reiterated in the next section for emphasis. Subsequent to Sela's papers was a paper by

Bestvina-Feighn [7], in which the authors took a more geometric approach to the same problem, and added a new, geometric definition of limit groups. It is the definition from [32] of finitely generated, fully residually free groups in the algebraic sense which we use in this thesis, as detailed in the next section.

4.1 Preliminaries

Recall, from Chapter 2, that limit groups are defined as finitely generated, fully residually free groups (Definition 2.3.4). There is another way to view these groups. It was shown in [32] that limit groups are precisely the finitely generated subgroups of the following iterated extension of centralisers.

Let G_0 be the free group generated by a finite set X_0, and for each $i \geq 1$ choose $w_i \in G_{i-1}$ to be an element with cyclic centraliser $C_{G_{i-1}}(w_i) = \langle w_i \rangle$, and let A_i be a free abelian group of rank k_i generated by the set

$$X_i := \{t_{i_1}, \ldots, t_{i_{k_i}}\}. \tag{4.1}$$

For $i = 1, \ldots, n$ set

$$G_i := G_{i-1} *_{\langle w_i \rangle} (\langle w_i \rangle \times A_i). \tag{4.2}$$

The set $X = \cup_{i=0}^{n} X_i$ is the canonical generating set for G_n. Throughout this chapter, we will use the notation

$$\mathcal{L}_X = \max\{\|a_i\|_X, \|b_i\|_X\} \tag{4.3}$$

where X is the generating set for G_n, and

$$\mathcal{L}_S = \max\{\|a_i\|_S, \|b_i\|_S\}, \tag{4.4}$$

where S is the generating set for a limit group G. When $G = G_n$ then $\mathcal{L}_S = \mathcal{L}_X$. An important constant used throughout this chapter is

$$\mathcal{M} = \max\{\|w_j\|_X;\ j = 1, \ldots, n\}. \tag{4.5}$$

Definition 4.1.1. Let G_n be a group as constructed in (4.2). An element $g \in G_n$ is called *conjugacy reduced* if it is minimal-length in its conjugacy class, i.e. for all $h \in G_n$ such that g is conjugate to h, $\|g\|_X \leq \|h\|_X$.

Lemma 4.1.2. *We can assume that the elements w_i from the construction (4.2) are conjugacy reduced.*

Proof. Let G_n be a group from construction (4.2), and suppose that this is true up to G_{k-1}, for $k \leq n$. Suppose that we amalgamate G_{k-1} over a subgroup generated by

w_k where w_k is not minimal length in its conjugacy class, according to construction (4.2) above:

$$G_{k-1} *_{\langle w_k \rangle} (\langle w_k \rangle \times A_k) \tag{4.6}$$

Let $\{t_1, \ldots, t_\ell\}$ be the generating set for A_k. Since w_k is not minimal-length in its conjugacy class, then

$$w_k = \gamma \overline{w_k} \gamma^{-1} \tag{4.7}$$

for some $\gamma \in G_{k-1}$, where $\overline{w_k}$ is minimal-length in its conjugacy class. Let $\overline{A_k}$ be a free abelian group generated by the set $\{\overline{t_1}, \ldots, \overline{t_\ell}\}$, and set

$$\overline{G_k} = G_{k-1} *_{\langle \overline{w_k} \rangle} (\langle \overline{w_k} \rangle \times \overline{A_k}). \tag{4.8}$$

The map $\phi : G_k \to \overline{G_k}$ which acts as the identity map when restricted to G_{k-1} and for each $j = 1, \ldots, \ell$ sends $\phi : t_j \mapsto \gamma \overline{t_j} \gamma^{-1}$ is an isomprphism. Note that

$$[\gamma \overline{t_j} \gamma^{-1}, w_i] = [\gamma \overline{t_j} \gamma^{-1}, \gamma \overline{w_i} \gamma^{-1}] = 1 \tag{4.9}$$

for $j = 1, \ldots, \ell$. □

Since the construction (4.2) is an amalgamated free product, elements of G_n can be written in their normal form in the following way. Choose transversals $T(G_{n-1})$ of shortest representatives for the right cosets of $\langle w_n \rangle$ in G_{n-1}. Each element $\gamma \in G_n$ can be written uniquely in the form

$$\gamma = g_0 \alpha_0 g_1 \ldots g_\nu \alpha_\nu \tag{4.10}$$

where $g_0 \in G_{n-1}$, $g_i \in T(G_{n-1})$ for all $i \geq 1$ and $\alpha_i \in A_n$ for all $i \geq 0$, such that $\alpha_i \neq 1$ for all $i < \nu$. We will sometimes use $\|\gamma\|_{NF}$ to denote the *length* $(:= \nu + 1)$ of the normal form of γ. In this chapter we will refer to the A_n*-shape* of an element. We say that an element $\gamma \in G_n$ has a *trivial* A_n-shape if $\gamma \in G_{n-1}$, otherwise γ has a *nontrivial* A_n-shape. We can talk about the t_k-shape being nontrivial if $t_k \in A_n$ occurs in the normal form of γ, trivial otherwise. This is directly analogous to the t-shapes in HNN extensions, and hence we can talk about A_n-reduction, meaning that there are some t_i terms (for some $t_i \in A_n$) which must cancel out in certain equations in G_n, as in the proof of Collins' Lemma (see, for example, [39]).

In order to use Collins' Lemma for amalgamated free products, we need elements to have *cyclically reduced normal forms*:

Definition 4.1.3. If the normal form $g_0 \alpha_0 g_1 \ldots g_\nu \alpha_\nu$ of γ is cyclically reduced, then either $\gamma \in G_{n-1}$, or $\gamma \notin G_{n-1}$ and $g_0 = 1$ if and only if $\alpha_\nu = 1$.

Remark 4.1.4. When we choose a conjugate $\overline{\gamma}$ of an element $\gamma \in G_n$ which has a cyclically reduced normal form, provided γ has a nontrivial A_n-shape, we can assume

that the final α-term (α_ν if the normal form is as written above) is nontrivial. For if it is trivial, then $g_\nu \overline{\gamma} g_\nu^{-1}$ ends with $\alpha_{\nu-1} \neq 1$, and we choose this conjugate instead.

Lemma 4.1.5. *Let $G = G_n$ be one of the groups from construction (4.2). If $A_i = g^{-1}A_j g$ for some $g \in G$, then $A_i = A_j$.*

Proof. Suppose that $i < j$ and $A_i = g^{-1}A_j g$ for some $g \in G$. If $t \in X_j$, then $gtg^{-1} \in A_i$ has a nontrivial A_j-shape, which is not possible. □

Theorem 4.1.6. *There exist increasing linear functions $f_0, \ldots, f_n$ such that, if*

$$w_k^{p_1} g = h w_\ell^{p_2} \tag{4.11}$$

is an equation in G_m for some m, then either $k = \ell$ and $g, h \in A_k \times \langle w_k \rangle$, or

$$\|w_k^{p_1}\|_X, \|w_\ell^{p_2}\|_X \leq f_m(\|g\|_X + \|h\|_X). \tag{4.12}$$

Proof. We argue by induction on m.

In the initial case, $m = 0$, the length $\|g\|_X$ is equal to the length of the reduced word in X_0 representing $g \in G_0 = \langle X_0 \rangle$. If

$$p_1 > \|g\|_X + \|h\|_X + \mathcal{M} \tag{4.13}$$

or

$$p_2 > \|g\|_X + \|h\|_X + \mathcal{M}, \tag{4.14}$$

after any cancellations the equation (4.11) gives rise to an equation

$$w_k^{\|w_\ell\|_X} = (\widetilde{w_\ell})^{\|w_k\|_X} \tag{4.15}$$

for some cyclic conjugate $\widetilde{w_\ell}$ of w_ℓ. If $k > \ell$ then it follows that $\langle w_k \rangle$ commutes in G_ℓ with some conjugate of an element of A_ℓ, which contradicts the group's construction. A similar contradiction arises if $\ell > k$, so $k = \ell$, which implies that $\widetilde{w_\ell} = w_\ell$. Since w_k generates its own centraliser in G_k it cannot be a proper power in the free group G_0. Thus equation (4.15) can be derived from equation (4.11) only if g and h are powers of w_k.

This completes the proof of the initial case of the induction, with

$$f_0(q) := \mathcal{M}(\mathcal{M} + q). \tag{4.16}$$

For the inductive step, suppose that we have found linear functions

$$f_0, \ldots, f_{m-1} \tag{4.17}$$

such that the conclusion of the theorem is true for equations in $G_0 \ldots, G_{m-1}$ respectively. We consider three subcases.

Case 1

Suppose that $w_k, w_\ell \in G_{m-1}$. If $g \in G_{m-1}$ then it follows from equation (4.11) that $h \in G_{m-1}$ and the result follows by induction. A similar remark applies if $h \in G_{m-1}$. We therefore assume that $g, h \notin G_{m-1}$.

Write $g = g_0 a_1 g_1 \cdots a_p g_p$ and $h = h_0 b_1 h_1 \cdots b_q h_q$ in normal form. Then $p > 0$, $q > 0$ and equation (4.11) in G_m implies that $p = q$ and that a system of equations

$$w_k^{p_1} g_0 = h_0 w_m^{\gamma(1)},\ w_m^{\gamma(1)} g_1 = h_1 w_m^{\gamma(2)},\ \cdots\ , w_m^{\gamma(p)} g_p = h_p w_\ell^{p_2} \tag{4.18}$$

holds in G_{m-1} for some $\gamma(1), \ldots, \gamma(p)$.

By inductive hypothesis we have

$$\begin{aligned} \|w_k^{p_1}\|_X &\leq f_{m-1}(\|g_0\|_X + \|h_0\|_X) \\ &\leq f_{m-1}(\|g\|_X + \|h\|_X), \end{aligned} \tag{4.19}$$

except possibly in the case where $k = m$ and $g_0, h_0 \in \langle w_m \rangle$.

Let us suppose that $k = m$ and $g_0, h_0 \in \langle w_m \rangle$. Unless $g, h \in \langle w_m \rangle \times A_m$ then by the construction of the normal form we have $g_1, h_1 \notin \langle w_m \rangle$, so

$$\begin{aligned} \|w_m^{\gamma(1)}\|_X &\leq f_{m-1}(\|g_1\|_X + \|h_1\|_X) \\ &\leq f_{m-1}(\|g\|_X + \|h\|_X) \end{aligned} \tag{4.20}$$

by inductive hypothesis. It follows that

$$\begin{aligned} \|w_k^{p_1}\|_X &\leq \|g_0\|_X + \|h_0\|_X + \|w_m^{\gamma(1)}\|_X \\ &\leq \|g\|_X + \|h\|_X + f_{m-1}(\|g\|_X + \|h\|_X). \end{aligned} \tag{4.21}$$

Finally, suppose that $g, h \in \langle w_m \rangle \times A_m$. Since $g, h \notin G_{m-1}$ then write $g = w_m^{q_1} \alpha_1$, $h = w_m^{q_2} \alpha_2$ where $q_1, q_2 \in \mathbb{Z}$ and $\alpha_1, \alpha_2 \in A_m \backslash \{1\}$. Then equation (4.11) together with the assumption that $w_k, w_\ell \in G_{m-1}$, gives the equation

$$(w_m^{q_2} w_\ell^{p_2})^{-1} \alpha_2^{-1} (w_k^{p_1} w_m^{q_1}) \alpha_1 = 1 \tag{4.22}$$

and we see that $\alpha_1 = \alpha_2$, and these A_m-terms must cancel. This leads to the conclusion that $w_k^{p_1}, w_\ell^{p_2} \in \langle w_m \rangle$. But $w_k^{p_1} \in \langle w_m \rangle$ if and only if either $p_1 = 0$ or $k = m$. Similarly $w_\ell^{p_2} \in \langle w_m \rangle$ if and only if either $p_2 = 0$ or $\ell = m$. If $p_1 = 0$ then $\|w_k^{p_1}\|_X = 0$ and

$\|w_\ell^b\|_X \leq \|g\|_X + \|h\|_X$. An analogous statement holds if $p_2 = 0$. Thus we are reduced to the case where $k = \ell = m$ and $g, h \in \langle w_m \rangle \times A_m$, as claimed.

Case 2

Suppose that $w_k \notin G_{m-1}$ but $w_\ell \in G_{m-1}$. (The argument for the case in which $w_\ell \notin G_{m-1}$ but $w_k \in G_{m-1}$ is similar.) In this case, any reduced word representing w_k must contain at least one letter from X_m. Since w_k has a cyclically reduced normal form with respect to the amalgamation (4.2), any reduced word representing $w_k^{p_1}$ must contain at least $|p_1|$ such letters which in the equation (4.11) must cancel with letters from g or h. It follows that $|p_1| \leq \|g\|_X + \|h\|_X$, so that $\|w_k^{p_1}\|_X \leq \mathcal{M}(\|g\|_X + \|h\|_X)$. Hence also

$$\begin{aligned} \|w_\ell^{p_2}\|_X &\leq \|g\|_X + \|w_k^{p_1}\|_X + \|h\|_X \\ &\leq (\mathcal{M}+1)(\|g\|_X + \|h\|_X). \end{aligned} \tag{4.23}$$

Case 3

Suppose that $w_k, w_\ell \notin G_{m-1}$. Then in particular $k > m$ so w_k generates its own centraliser in G_m, and so w_k is not an element of $\langle w_m \rangle \times A_m$. Similarly w_ℓ is not an element of $\langle w_m \rangle \times A_m$.

As in Case 1, we write

$$g = g_0 a_1 \cdots a_p g_p \quad \text{and} \quad h = h_0 b_1 \cdots b_q h_q \tag{4.24}$$

in normal form, noting that $p \leq \|g\|_X$ and $q \leq \|h\|_X$. By Remark 4.1.4, we can also write $w_k = c_1 u_1 \cdots c_r u_r$, $w_\ell = d_1 v_1 \cdots d_s v_s$, where $r > 0$, $s > 0$, $c_i, d_i \in A_m \smallsetminus \{1\}$, and $u_i, v_i \in G_{m-1} \smallsetminus \langle w_m \rangle$ for $i > 1$. Again $r \leq \|w_k\|_X \leq \mathcal{M}$ and $s \leq \|w_\ell\|_X \leq \mathcal{M}$.

Now suppose that

$$p_1 > \|g\|_X + \|h\|_X + \mathcal{M} + 1 \geq p + q + s + 1. \tag{4.25}$$

Then in equation (4.11) there is a subword of $w_k^{p_1}$ equal to w_k^{s+1} in which the X_m letters cannot cancel with those in g or h, so must cancel with some of those in $w_\ell^{p_2}$. In particular there is a sequence of $rs + 1$ equations in G_{m-1} of the form

$$c_1 w_m^{\gamma(1)} = w_m^{\gamma(0)} d_K,\ c_2 w_m^{\gamma(2)} = w_m^{\gamma(1)} d_{K+1},\ \ \ldots,\ c_{rs+1} w_m^{\gamma(rs+1)} = w_m^{\gamma(rs)} d_{K+rs} \tag{4.26}$$

for some K and some $\gamma(i)$, where the c-subscripts are interpreted modulo r and the d-subscripts modulo s. In particular $c_{rs+1} = c_1$ and $d_{K+rs} = d_K$. Hence

$$c_1 w_m^{\gamma(rs+1)-\gamma(1)} c_1^{-1} = w_m^{\gamma(rs)-\gamma(0)}. \tag{4.27}$$

Since $c_1 \notin \langle w_m \rangle$ and $\langle w_m \rangle$ is self-normalising, this is possible only if $\gamma(rs+1) = \gamma(1)$ and $\gamma(rs) = \gamma(0)$. Hence

$$w_m^{-\gamma(0)} w_k^s w_m^{\gamma(0)} = (\widetilde{w_\ell})^r, \tag{4.28}$$

where

$$\widetilde{w_\ell} = d_K v_K \cdots d_s v_s d_1 v_1 \cdots d_{K-1} v_{K-1} \tag{4.29}$$

is the cyclic conjugate of w_ℓ beginning with d_K.

If $k < \ell$, this means that some conjugate of A_k commutes with w_ℓ in $G_{\ell-1}$, contrary to the hypothesis that w_ℓ generates its own centraliser. A similar contradiction occurs if $k > \ell$. Hence $k = \ell$. Moreover, $w_\ell = w_k$ commutes with $w_m^{\gamma(0)} d_k v_k \cdots d_s v_s$ in G_m Since $\langle w_\ell \rangle$ is self-centralising, this is possible only when $k = 1$ and $\gamma(0) = 0$. In other words, the equation (4.11) exactly matches up some copies of w_k in $w_k^{p_1}$ with copies of $w_k = w_\ell$ in $w_\ell^{p_2}$. This in turn is possible only if $g, h \in \langle w_k \rangle$.

Hence either $k = \ell$ and $g, h \in \langle w_k \rangle$, or

$$\|w_k^{p_1}\|_X \leq |p_1| \cdot \|w_k\|_X \leq (\|g\|_X + \|h\|_X + \mathcal{M} + 1) \cdot \mathcal{M}. \tag{4.30}$$

Similar arguments apply to $\|w_\ell^{p_2}\|_X$.

□

Theorem 4.1.7. *There exists a linear function L such that, for all integers $0 < p < q$ and for all $g \in G_n$,*

$$\|g^p\|_X \leq L(\|g^q\|_X). \tag{4.31}$$

Proof. Induction on n. If $n = 0$ then G_n is free and the given generating set is a basis. The result is true with respect to the linear function $L(x) := x$.

Assume that the result is true for G_{n-1} with respect to the linear function L'. Let $g \in G_n$, $0 < p < q$ and let W be a word in the standard generators representing g^q. Then by Remark 4.1.4 there exists a cyclic conjugate $\overline{W}$ of W representing a conjugate $\overline{g}^q$ of g^q, such that one of the following is true:

1. $\overline{g}^q \in G_{n-1}$;
2. $\overline{g}^q \in A_n \times \langle w_n \rangle$;
3. $\overline{g}^q = g_1 \alpha_1 \cdots g_k \alpha_k$ in cyclically reduced normal form. and $\alpha_j \in A_n \setminus \{1\}$ for each $j = 1, \ldots, k$.

In the first case, $\overline{g} \in G_{n-1}$. By inductive hypothesis $\|\overline{g}^p\|_X \leq L'(\|\overline{g}^q\|_X) \leq L'(|W|)$. Hence

$$\|g^p\|_X \leq |W| + L'(|W|) = \|g^q\|_X + L'(\|g^q\|_X). \tag{4.32}$$

In the second case, $\overline{g} \in A_n \times \langle w_n \rangle$. Say $\overline{g} = \alpha w_n^t$ where $\alpha \in A_n$. Then

$$\|\overline{g}^q\|_X = q\|\alpha\|_X + \|w_n^{tq}\|_X. \tag{4.33}$$

Hence, by inductive hypothesis,

$$\|\overline{g}^p\|_X = p\|\alpha\|_X + \|w_n^{tp}\|_X \leq p\|\alpha\|_X + L'(\|w_n^{tq}\|_X). \tag{4.34}$$

Thus

$$\begin{aligned}
\|g^p\|_X &\leq |W| + p\|\alpha\|_X + L'(\|w_n^{tq}\|_X), \text{ by Equation 4.34} \\
&\leq |W| + q\|\alpha\|_X + L'(\|w_n^{tq}\|_X), \text{ since } p < q \\
&\leq |W| + \|\overline{g}^q\|_X + L'(\|\overline{g}^q\|_X), \text{ since } \overline{g} \text{ is cyclically reduced} \\
&\leq 2\|g^q\|_X + L'(\|g^q\|_X). \qquad (4.35)
\end{aligned}$$

In the third case, the expression

$$\overline{g}^q = g_1\alpha_1 \cdots g_k\alpha_k \tag{4.36}$$

for $\overline{g}^q$ is cyclically reduced with respect to the amalgamated free product decomposition $G_n = G_{n-1} *_{\langle w_m \rangle} (A_n \times \langle w_n \rangle)$. Hence $\overline{g}$ is also cyclically reduced with respect to this decomposition, so $k = qs$ for some positive integer s. Moreover

$$\overline{g}^p = g_1\alpha_1 \cdots g_{ps}\alpha_{ps}w_n^t \tag{4.37}$$

for some integer t. Now define

$$\overline{h} = g_{ps+1}\alpha_{ps+1} \cdots g_k\alpha_k g_1\alpha_1 \cdots g_{ps}\alpha_{ps}. \tag{4.38}$$

Then $\|\overline{h}\|_X \leq \|g^q\|_X$ and $\overline{h} = w_n^t\overline{g}^q w_n^{-t}$. It follows that

$$\|w_n^t\|_X \leq f_n(\|\overline{g}^q\|_X + \|\overline{h}\|_X) \tag{4.39}$$

where f_n is the linear function of Theorem 4.1.6. Hence

$$\begin{aligned} \|g^p\|_X &\leq |W| + \|\overline{g}^p\|_X \\ &\leq |W| + \|\overline{g}^q\|_X + \|w_n^t\|_X, \text{ by Equation 4.37} \\ &\leq 2\|\overline{g}^q\|_X + f_n(\|\overline{g}^q\|_X + \|\overline{h}\|_X), \text{ by Equation 4.39} \\ &\leq 2\|\overline{g}^q\|_X + f_n(2\|g^q\|_X). \end{aligned} \tag{4.40}$$

□

4.2 Conjugacy search problem

Lemma 4.2.1. *Let $G = G_n$ be a group from construction (4.2). Suppose that a, b are conjugate elements in G which both have a cyclically reduced normal form in the sense of Remark 4.1.4. Then there is an element $x \in G$ such that $x^{-1}ax = b$ and $\|x\|_X$ has a linear bound in $\mathcal{L}_X$.*

Proof. Suppose that a has a trivial G_n-normal form – in other words, $a \in G_{n-1}$. Then b is also an element of G_{n-1}, and we use induction on n. If a is an element of $(A_n \times \langle w_n \rangle)$ then so is b, and $a = b$, so the identity element is the required conjugator.

Now suppose that $a, b \notin G_{n-1}$ and $a, b \notin (A_n \times \langle w_n \rangle)$. By Theorem 4.6 of [40], called "The Conjugacy Theorem for Free Products with Amalgamation", we know that b can be obtained from a by cyclically permuting a and then conjugating the result, $\overline{a}$, by a power of w_n: write $b = w_n^{-k}\overline{a}w_n^k$. By Theorem 4.1.6, there is a linear bound on $\|w_n^k\|_X$. Hence $\|x\|_X \leq Q \cdot \mathcal{L}$ for some integer Q. □

Corollary 4.2.2. *Let G_n be a group from construction (4.2). Then there exists an integer Q such that for any two conjugate elements $a, b \in G_n$, there exists $x \in G_n$ such that $x^{-1}ax = b$ and $\|x\|_X \leq Q \cdot \mathcal{L}_X$.*

Proof. We can cyclically permute a to the element $\overline{a}$ with cyclically reduced normal form (the same cyclic permutation $\overline{a}$ required to apply Lemma 4.2.1) using a subword τ_1 of a. Likewise we can cyclically permute b to $\overline{b}$ using a subword τ_2 of b. By Lemma 4.2.1, it now follows that there is an element x which conjugates a to b and has linearly bounded length $\|x\|_X \leq Q\mathcal{L}_X$. □

Corollary 4.2.3. *Let G_n be a group from construction (4.2). Then there is a linear function $f : \mathbb{N} \to \mathbb{N}$ such that for any element $a \in G_n$, there exists a subset $S_a \subset G_n$ such that S_a generates the centraliser $C_{G_n}(a)$, and for each $s \in S_a$, $\|s\|_X \leq f(\|a\|_X)$.*

Proof. First suppose that a has a cyclic centraliser. If a generates its own centraliser then this corollary is clearly correct. If a is a proper power of an element u which generates the centraliser of a, then $a = u^k$ for some $k \in \mathbb{Z}$ and $\|u\|_X \leq L(u^k)$ by Theorem 4.1.7.

If a has a non-cyclic centraliser then either $C_{G_n}(a) = A_k \times \langle w_k \rangle$ for some $k \in \mathbb{Z}$ or it is a conjugate $g^{-1}(A_k \times \langle w_k \rangle)g$ for some $g \in G_n$. The subgroup $A_k \times \langle w_k \rangle$ is generated by the set $X_k \cup \{w_k\}$, as explained at the beginning of this chapter, and $\|w_k\|_X$ is bound by the constant $\mathcal{M} = \max\{\|w_i\|_X, i = 1, \ldots, n\}$ which is dependent on the choice of group G_n.

In the case where the centraliser of a is a conjugate of $A_k \times \langle w_k \rangle$, we have

$$a = g^{-1}ug \tag{4.41}$$

where $u \in A_k \times \langle w_k \rangle$.

Since elements of $A_k \times \langle w_k \rangle$ are conjugacy-reduced by Lemma 4.1.2, it is clear that $\|u\|_X \leq \|a\|_X$. Thus we can use Corollary 4.2.2 with Equation (4.41) to find a linear length bound on $\|g\|_X$. As a consequence any generating element of $C_{G_n}(a)$ is of the form $g^{-1}vg$, where v, a generator of $(A_k \times \langle w_k \rangle)$, is bounded by a constant according to the choice of group G_n. Using the triangle inequality,

$$\|g^{-1}vg\|_X \leq 2\|g\|_X + \|v\|_X \tag{4.42}$$

gives a linear bound on the size of the generators of the centraliser of a. □

Theorem 4.2.4. *Let G be a limit group with generating set S. Then there exists an integer P such that for any two conjugate elements $a, b \in G$, there exists an element $x \in G$ such that $x^{-1}ax = b$ and*

$$\|x\|_S \leq P \max\{\|a\|_S, \|b\|_S\}. \tag{4.43}$$

Proof. Lemma 4.2.2 shows this to be true if $G = G_n$ for some n. Otherwise G is a proper subgroup of some G_n. Suppose that we have found, using Corollary 4.2.2, that there is an element $c \in G_n$ such that $c^{-1}ac = b$ and $\|c\|_S$ is bounded above by a linear function of $\mathcal{L}$. Then the set

$$Z = \{zc \ : \ z \in C_{G_n}(a)\} \tag{4.44}$$

is the set of all elements which conjugate a to b in G_n, and $Z \cap G$ is the set of all elements which conjugate a to b in G.

Suppose that a has a cyclic centraliser in G_n, say $C_{G_n}(a) = \langle \alpha \rangle$ with $a = \alpha^\lambda$ for some $\lambda \in \mathbb{Z}$. Then $C_G(a) = \langle \alpha^d \rangle$ for some divisor d of λ. Given $c \in Z$ (the same c as

above), there is some integer q with $|q| \leq \frac{d}{2}$, such that $\alpha^q c \in G$. Then $\alpha^q c \in Z \cap G$ and

$$\begin{aligned} \|\alpha^q c\|_X &\leq \|\alpha^q\|_X + \|c\|_X \\ &\leq L\|\alpha^\lambda\|_X + \|c\|_X, \text{ by Theorem 4.1.7} \\ &= \|a\|_X + \|c\|_X \end{aligned} \tag{4.45}$$

for some integer L. Using the distortion result in Lemma 2.4.8 gives a bound on $\|\alpha^q c\|_S$ which is linear in $\mathcal{L}_S$.

Now suppose that a and b have non-cyclic centralisers in G_n – call these

$$\gamma_a^{-1}(\langle w_{\lambda_a}\rangle \times A_{\lambda_a})\gamma_a \text{ and } \gamma_b^{-1}(\langle w_{\lambda_b}\rangle \times A_{\lambda_b})\gamma_b \tag{4.46}$$

respectively. By Lemma 4.1.5 we know that $\lambda_a = \lambda_b$. Either $\lambda_a = n$ or $(\langle w_{\lambda_a}\rangle \times A_{\lambda_a}) \leq G_{n-1}$. In terms of the Bass-Serre tree T of the splitting $G_n = G_{n-1} *_{\langle w_n\rangle} (\langle w_n\rangle \times A_n)$, this means that each of a, b fixes a vertex. In turn, Bass-Serre theory translates the action of G on T into a graph-of-groups decomposition of G, in which each of a, b is conjugate in G to an element $\breve{a}$, $\breve{b}$ of a vertex group $\Gamma_u :=\text{Stab}_G(u)$, $\Gamma_v :=\text{Stab}_G(v)$ respectively. Since $\breve{a} = g\breve{b}g^{-1}$ for some $g \in G$, then $\breve{a}$ fixes the vertices u and $g(v)$ in T.

If neither $\breve{a}$ nor $\breve{b}$ fixes a vertex whose stabiliser is conjugate to a subgroup of $\langle w_n\rangle \times A_n$ (for brevity, call such vertices A_n-vertices) then they fix vertices whose stabilisers are conjugates of subgroups of G_{n-1} (just call these "G_{n-1}-vertices" for short). If $u \neq g(v)$ then the action of $\breve{a}$ fixes a path in T and hence it fixes an edge. Since the edge stabilisers are conjugates of $\langle w_n\rangle$, this implies that $\breve{a}$ also fixes an A_n-vertex, which is a contradiction. If $u = g(v)$ then $\Gamma_u = \Gamma_v$, so $g \in \Gamma_u$, and we use induction to look at the action of $\breve{a}, \breve{b}$ on the Bass-Serre tree for G_{n-1}.

Suppose that $\breve{a}, \breve{b}$ both fix A_n-vertices. If $u \neq g(v)$ then $\breve{a}$ fixes a path of length at most 2 (since the action of G_n and hence of G is 2-acylindrical on T – see [49]). This path cannot have length 1, because that would imply that there are two A_n-vertices adjacent in T. Thus $\breve{a}$ fixes the path $u, z, g(v)$ with edges e, e' respectively, and z is a G_{n-1}-vertex. The stabiliser of the edge e in G is a subgroup of $\text{Stab}_{G_n}(e) = h\langle w_n\rangle h^{-1}$ for some $h \in G_n$, and this is malnormal in $\text{Stab}_{G_n}(z) = hG_{n-1}h^{-1}$. Since $\text{Stab}_{G_n}(z)$ acts transitively on the edges incident to z, there is some $\gamma \in \text{Stab}_{G_n}(z)$ such that $\gamma(e) = e'$. It follows that

$$\gamma h\langle w_n\rangle h^{-1}\gamma^{-1} = \text{Stab}_{G_n}(e'). \tag{4.47}$$

By malnormality,

$$h\langle w_n\rangle h^{-1} \cap \gamma h\langle w_n\rangle h^{-1}\gamma^{-1} = \{1\}, \tag{4.48}$$

but $\breve{a}$ is a nontrivial element of this intersection, which is a contradiction. Thus $u = g(v)$, so $\breve{a}, \breve{b}$ both belong to the same A_n-vertex, and so $\breve{a} = \breve{b}$.

It remains to take account of the fact that we have replaced a, b by conjugates $\breve{a}, \breve{b}$. Provided we choose the generating set for G sensibly (say the union of finite generating sets of each of the vertex groups, together with a finite set of stable letters) then we can choose $\breve{a}, \breve{b}$ to be cyclic conjugates of a, b, and so

$$\|x\|_S \leq \|a\|_S + \|b\|_S. \tag{4.49}$$

□

4.3 Multiple conjugacy search problem

It turns out that the multiple conjugacy search problem also has a linear bound in limit groups. In fact, the problem can be simplified by making use of the fact that limit groups are commutative-transitive (see [3]).

It follows, by Remark 4 of [44], that G has the "SA property", defined as follows:

Definition 4.3.1. A group G is said to have the *SA property* if distinct maximal abelian subgroups of G intersect trivially.

Lemma 4.3.2. *Let G be a commutative-transitive group, and let $A = [a_1, \ldots, a_m]$ and $B = [b_1, \ldots, b_m]$ be conjugate lists of elements in G. Then with suitable renumbering of the lists, the multiple conjugacy search problem for A and B can be reduced to either $A' = [a_1, a_2]$ and $B' = [b_1, b_2]$, in which case there is a unique solution. Otherwise the multiple conjugacy search problem is reduced to the conjugacy search problem for a_1 and b_1.*

Proof. If there is an element $x \in G$ such that $A^x = B$ then all solutions to the generalised conjugacy search problem for A and B are of the form cx, where $c \in \bigcap_i C_G(a_i)$. Since G is commutative-transitive then the centraliser of every nonidentity element is a maximal abelian subgroup of G. Furthermore since G has SA property, it follows that either there are two elements which we reorder as a_1, a_2 in A with trivially intersecting centralisers, in which case the multiple conjugacy search problem is reduced to finding the unique solution to the multiple conjugacy search problem for $A' = [a_1, a_2]$ and $B' = [b_1, b_2]$. Otherwise the centralisers for every element in A are identical, and so the multiple conjugacy search problem is reduced to finding an element which conjugates a_i to b_i for any i. □

Remark 4.3.3. Let G_n be a group from the construction (4.2) and let $a, b \in G_n$ be elements with cyclic centralisers such that $x^{-1}ax = b$ for some $x \in G_n$. We may assume for the purposes of the conjugacy search problem that $C_{G_n}(a) = \langle a \rangle$. For if $a = u^k$ for some $u \in G$ and $k \in \mathbb{Z}$ then

$$b = x^{-1}u^k x = (x^{-1}ux)^k = v^k, \tag{4.50}$$

and any element which conjugates a to b will conjugate u to v. Furthermore, Theorem 4.1.7 tells us that there is an integer L such that $\|u\|_X \leq L(\|u^k\|)$, so we have $\|u\|_X$ bounded linearly in terms of $\|a\|_X$. Hence we can assume that a is not a proper power of any other element.

For the final theorem, we need a refined version of Theorem 4.1.6, namely:

Theorem 4.3.4. *There exist increasing linear functions $f_0, \ldots, f_n$ such that, if*

$$u^k g = hu^k \tag{4.51}$$

is an equation in G_m for some m, where $u \in G_m$ generates its own centraliser, then either $g, h \in \langle u \rangle$, or

$$\|u^k\|_X \leq f_m(\|g\|_X + \|h\|_X). \tag{4.52}$$

Proof. As in Theorem 4.1.6, the argument is by induction on m.

In the initial case, $m = 0$, the length $\|g\|_X$ is equal to the length of the reduced word in X_0 representing $g \in G_0 = \langle X_0 \rangle$. If $k > \|g\|_X + \|h\|_X + 1$ then after any cancellations, equation (4.51) produces an equation

$$u = \tilde{u}, \tag{4.53}$$

where $\tilde{u}$ is a cyclic conjugate of u. Since u is an element which generates its own centraliser in G_m, and is therefore not a proper power of any other element, then this implies that equation (4.53) can only be derived from equation (4.51) if g and h are powers of u.

This completes the proof of the initial case of the induction, with

$$f_0(q) := \mathcal{M}q. \tag{4.54}$$

For the inductive step, suppose that we have found linear functions

$$f_0, \ldots, f_{m-1} \tag{4.55}$$

such that the conclusion of the theorem is true for equations in $G_0 \ldots, G_{m-1}$ respectively. We consider two subcases.

Case 1: $u^k \in G_{m-1}$.

By equation (4.51) it follows that $h \in G_{m-1}$ if and only if $g \in G_{m-1}$, and the result follows by induction. We therefore assume that $g, h \notin G_{m-1}$.

Equation (4.51) in G_m implies that g and h have the same normal form length. Write

$$g = g_0 a_1 g_1 \cdots a_p g_p \text{ and } h = h_0 b_1 h_1 \cdots b_p h_p \tag{4.56}$$

in normal form, with $p > 0$. Equation (4.51) further implies that that a system of equations

$$u^k g_0 = h_0 w_m^{\gamma(1)},\ w_m^{\gamma(1)} g_1 = h_1 w_m^{\gamma(2)},\ \ \ldots\ , w_m^{\gamma(p)} g_p = h_p u^k \tag{4.57}$$

holds in G_{m-1} for some $\gamma(1), \ldots, \gamma(p)$, and that $a_i = b_i$ for $i = 1, \ldots, p$, and so the equation

$$w_m^{\gamma(1)} g_1 a_2 \ldots a_p g_p g_0 = h_1 b_2 \ldots b_p h_p h_0 w_m^{\gamma(1)} \tag{4.58}$$

also holds. Theorem 4.1.6 gives a bound on $\|w_m^{\gamma(1)}\|_X$ which is a linear function over $\|g\|_X, \|h\|_X$. Hence

$$\|u^k\|_X = \|h_0 w_m^{\gamma(1)} g_o^{-1}\|_X \tag{4.59}$$

is also bounded by a linear function of $\|g\|_X, \|h\|_X$.

Case 2: $u^k \notin G_{m-1}$.

As in Case 1, we write

$$g = g_0 a_1 \cdots a_p g_p,$$

$$h = h_0 b_1 \cdots b_q h_q \tag{4.60}$$

in normal form, noting that $p \leq \|g\|_X$ and $q \leq \|h\|_X$. By Remark 4.1.4, we can also write

$$u = c_1 u_1 \cdots c_r u_r, \tag{4.61}$$

where $r > 0$, $c_i \in A_m \smallsetminus \{1\}$, and $u_i \in G_{m-1} \smallsetminus \langle w_m \rangle$ for $i > 1$. Again $r \leq \|w_k\|_X \leq \mathcal{M}$. The argument which follows, expressed algebraically, is illustrated with a cancellation diagram in Figure 4.3. For some i, j with $i + j = p + q$, there are equations

$$h_0 w_m^{\alpha_1} = u_1,\ h_1 w_m^{\alpha_2} = w_m^{\alpha_1} u_2,\ \ \ldots\ ,\ h_{j-1} w_m^{\alpha_j} = w_m^{\alpha_{j-1}} u_j, \tag{4.62}$$

$$h_j w_m^{\alpha_{j+1}} u_{q-j+1} = w_m^{\alpha_j} u_{j+1} w_m^{\gamma_1}, \tag{4.63}$$

$$w_m^{\gamma_1} u_{q-j+2} = u_{j+2} w_m^{\gamma_2},\ \ \ldots\ ,\ w_m^{\gamma_{kr-i-2j+1}} u_{kr+q-i-2j-1} = u_{kr-i-1} w_m^{\gamma_{kr-i-2j+2}}, \tag{4.64}$$

$$u_{kr-i} w_m^{\beta_i} g_i = w_m^{\gamma_{kr-i-2j+2}} u_{kr+q-i-2j} w_m^{\beta_{i+1}}, \tag{4.65}$$

$$u_{kr+q-i-2j+1} w_m^{\beta_{i+2}} = w_m^{\beta_{i+1}} g_{i+1},\ \ \ldots\ ,\ u_{kr-1} w_m^{\beta_{p-1}} g_{p-1},\ u_{kr} = w_m^{\beta_p} g_p. \tag{4.66}$$

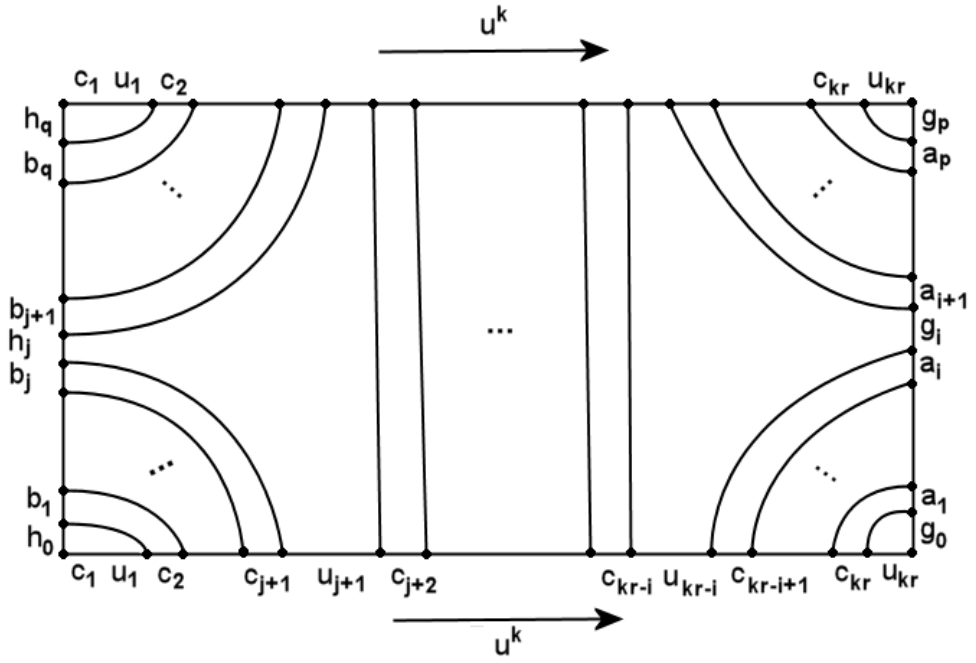

Figure 4.1: Cancellation diagram for Theorem 4.3.4

If the middle section contains more than r strips linking u_j-symbols (i.e. if $kr - p - q - 3 \geq r + 1$), then there is a sequence of $r + 1$ equations in G_{m-1} of the form

$$u_1 w_m^{\gamma(1)} = w_m^{\gamma(0)} u_K,\ u_2 w_m^{\gamma(2)} = w_m^{\gamma(1)} u_{K+1},\ \ \ldots\ ,\ u_{r+1} w_m^{\gamma(r+1)} = w_m^{\gamma(r)} u_{K+r} \qquad (4.67)$$

for some $K \in \mathbb{Z}$ and some $\gamma(i)$, where the c-subscripts are interpreted modulo r. In particular $u_{r+1} = u_1$ and $u_{K+r} = u_K$. Hence

$$u_1 w_m^{\gamma(r+1)-\gamma(1)} u_1^{-1} = w_m^{\gamma(r)-\gamma(0)}. \qquad (4.68)$$

Since $c_1 \notin \langle w_m \rangle$ and $\langle w_m \rangle$ is self-normalising, this is possible only if $\gamma(r+1) = \gamma(1)$ and $\gamma(r) = \gamma(0)$. Hence

$$w_m^{-\gamma(0)} u w_m^{\gamma(0)} = \tilde{u}, \qquad (4.69)$$

where

$$\widetilde{u} = c_K v_K \cdots c_r v_r c_1 v_1 \cdots c_{K-1} v_{K-1} \qquad (4.70)$$

is the cyclic conjugate of u beginning with c_K.

This implies that u commutes with $w_m^{\gamma(0)} c_K v_K \cdots d_r v_r$ in G_m. Since $\langle u \rangle$ is self-centralising, this is possible only when $K = 1$ and $\gamma(0) = 0$. In other words, the equation (4.51) exactly matches up some copies of u in u^k on each side of the equation (4.51) with copies of u in u^k on the opposite side of the equation (4.51). This in turn is possible only if $g, h \in \langle u \rangle$.

Now suppose that there are at most r equations as in (4.67) - in other words, there

are only r strips in the "middle section" in Figure 4.3. Write u^k as a product $x \cdot y \cdot z$ where the middle section

$$y = u_{j+1}c_{j+2}u_{j+2}\cdots c_{kr-i}u_{kr-i} \tag{4.71}$$

is a subword of a cyclic conjugate of u^4 by the assumed inequality $(kr-i)-j \leq r+3$, and so has length at most $4||u||_X$. Now

$$x = h_0 b_1 \cdots h_{j-1} b_j w_m^{\alpha_j}, \tag{4.72}$$

where $||w_m^{\alpha_j}||_X$ is bounded above by a linear function of $||h||_X$ and $||u||_X$ – by Theorem 4.1.6 applied to the equation

$$h_{j-1} w_m^{\alpha_j} = w_m^{\alpha_{j-1}} u_j \tag{4.73}$$

if $j > 1$, or since $w_m^{\alpha} = h_0^{-1} c_1 u_1$ if $j = 1$. Hence $||x||_X \leq ||h||_X + ||w_m^{\alpha}||_X$ is also bounded above by a linear function of $\|h\|_X$ and $||u||_X$. Similarly $||z||_X$ is bounded above by a linear function of $||g||_X$ and $||u||_X$. Hence $||u^k||_X \leq ||x||_X + ||y||_X + ||z||_X$ is bounded above by a linear function of $||g||_X$, $||h||_X$ and $||u||_X$.

Hence either $g, h \in \langle u \rangle$, or $\|u^k\|_X$ is bounded above by a linear function of $||g||_X$ and $||u||_X$. □

Now that we can solve the conjugacy search problem in limit groups, and we have managed to reduce the multiple conjugacy search problem to a list of two elements, we are ready to prove the main theorem:

Theorem 4.3.5. *Let G be a limit group with generating set S. Then there is a linear function $F : \mathbb{N} \to \mathbb{N}$ such that for any two finite lists $A = [a_1, \ldots, a_m]$, $B = [b_1, \ldots, b_m]$ which are conjugate in G (with $\mathcal{L} = \max\{\|a_i\|_X, \|b_i\|_X, i = 1, \ldots, m\}$), there exists $x \in G$ such that $x^{-1}a_i x = b_i$ for $i = 1, \ldots, n$, and $\|x\|_S \leq F(\mathcal{L})$.*

Proof. Since limit groups are commutative-transitive, we can use Lemma 4.3.2 so that, after suitable rearranging of the lists, we can identify A, B with lists of length $m = 1$ or $m = 2$. If $m = 1$ then Proposition 4.2.4 gives the required linear bound. Otherwise we assume that $m = 2$, and that $C_G(a_1) \cap C_G(a_2) = \{1\}$.

We begin with the case that G is one of the groups G_n described in (4.2), and recall that this group can be viewed as an amalgamated product, and that $S = X$.

If a_1 has a cyclic centraliser, generated by some element $u \in G_n$, then $\|u\|_X$ is bounded above by a linear function of $\|a_1\|_X$ by Theorem 4.1.7. We can apply Corollary 4.2.2 to find an element $c \in G_n$, whose length is bounded by a linear function of $\mathcal{L}$, such that $a_1 = c^{-1}b_1 c$. The element which conjugates a_2 to b_2 will have

the form $x = u^k c$ for some $k \in \mathbb{Z}$. If we write $\overline{b_2} = c^{-1} b_1 c$ then we can form the equation $u^{-k}\overline{b_2}u^k = a_2$, or in a more familiar guise:

$$\overline{b_2}u^k = u^k a_2 \tag{4.74}$$

Applying Theorem 4.3.4 to equation (4.74), we find an upper bound for the length of u^k which is linear in $\mathcal{L}$. Consequently the length of the required element x is bounded above by a linear function of $\mathcal{L}$. An analogous argument applies if a_2 has a cyclic centraliser.

If a_1 and a_2 both have non-cyclic centralisers then, as noted in Lemma 4.2.4, they both fix vertices in the Bass-Serre tree of G_n.

If they do not fix the same vertex then $a_1 a_2$ does not fix a vertex, which implies that $C_{G_n}(a_1 a_2)$ is cyclic. We can then apply the above argument to the lists $A' = [a_1 a_2, a_2]$, $B' = [b_1 b_2, b_2]$, since any element which conjugates a_1 to b_1 and a_2 to b_2 will conjugate $a_1 a_2$ to $b_1 b_2$.

If a_1 and a_2 fix the same vertex in the Bass-Serre tree, then this must be a G_{n-1}-vertex, otherwise a_1 and a_2 share the same centraliser, as explained in Lemma (4.2.4), which is a contradiction. It follows that a_1 and a_2 belong to some conjugate of G_{n-1}, and we can use induction on n to complete the argument.

We conclude that for $G = G_n$ there is some x with a length bound $\|x\|_X$ which is linear in $\mathcal{L}_X$.

The remaining possibility is that G is a proper subgroup of G_n for some n. Recall that a consequence of the commutative-transitive property is that the solution to the multiple conjugacy search problem when $m = 2$ is unique. Since G is a subgroup of G_n, the element which conjugates A to B in G is the same element which conjugates A to B in G_n. Combining this with Lemma 2.4.8 we conclude that the solution to the multiple conjugacy search problem in limit groups has a linear upper bound. □

Chapter 5

Finitely presented residually free groups

The multiple conjugacy problem (a decision problem: given two lists of elements in a group, decide whether they are conjugate) for finitely presented residually free groups was solved in [14]. In this chapter we show that the multiple conjugacy search problem in finitely presentable residually free groups has a polynomial length bound.

Wall [54] and Serre [50] pioneered the study of higher finiteness properties of groups. Stallings [52] gave the first example of a finitely presentable group whose third integral homology group is not finitely generated. This group was a subgroup of $F_2 \times F_2 \times F_2$, the direct product of three free groups of rank 2. Bieri [9] showed that Stallings' group belongs to a sequence of groups SB_n, called *Stallings-Bieri groups*, which display similar "bizarre" homological behaviour.

In the same spirit, Miller [42] and Mihaĭlova [41] gave an example of a finitely generated subgroup of $F_2 \times F_2$ with undecidable conjugacy and membership problems. It is fairly straightforward to construct examples of finitely generated subgroups with unsolvable decision problems inside apparently well-behaved groups (further examples seen in [4], [43], [48]). It is not so easy to find such finitely presentable subgroups.

In [5] Baumslag et. al. find a set of finitely presented subgroups of automatic groups which satisfy, at best, an exponential isoperimetric inequality. In a subsequent paper [6], the same authors show that there exists a finitely presented group P in a biautomatic group G for which the generalised word problem and conjugacy problem are unsolvable. In this paper, the authors provide a criterion for a fibre product to be finitely presentable – this is known as the 1-2-3 Theorem:

Theorem 5.0.6 (1-2-3 Theorem [5])**.** *Suppose that*

$$1 \to N \to \Gamma \to Q \to 1 \tag{5.1}$$

is an exact sequence with N finitely generated, G finitely presented and Q of type F_3.

Then the associated fibre product

$$P = \{(g, h) \ : \ p(g) = p(h)\}, \tag{5.2}$$

where $p : G \to Q$ is the homomorphism in the exact sequence, is finitely presented.

It was shown in [14] that finitely presentable residually free groups, viewed as subgroups of direct products of limit groups, have a solvable conjugacy problem. This is not necessarily true for residually free groups which are finitely generated but not finitely presentable. For example:

Example 5.0.7. Let $F_2 \times F_2$ be the direct product of two free groups of rank 2. Then there exists a subgroup of $F_2 \times F_2$ for which the conjugacy problem is unsolvable.

Proof. The solubility of the word problem is closed under taking subgroups, and every group is the subgroup of a 2-generated group. Therefore there exists a 2-generated finitely presented group G with unsolvable word problem:

$$G := \langle x, y \mid r_1, \ldots, r_n \rangle. \tag{5.3}$$

Using this presentation we define H to be the subgroup of $F_2 \times F_2$ generated by the set

$$\{(x, x), (y, y), (r_1, 1), \ldots, (r_n, 1)\}. \tag{5.4}$$

Choose an element $(w, 1) \in F_2 \times F_2$, and define

$$a := (r_1, r_1) \text{ and } b := (w^{-1}, 1)(r_1, r_1)(w, 1). \tag{5.5}$$

We can assume that r_1 is not a proper power. Since

$$b = (w^{-1} r_1 w, r_1) = (r_1, r_1)(r_1^{-1} w^{-1} r_1 w, 1) \tag{5.6}$$

then $b \in H$, as $r_1^{-1} w^{-1} r_1 w = 1$ in G. So a, b are two elements of H which are conjugate in G. Furthermore,

$$C_{F_2 \times F_2}(a) = C_{F_2}(r_1) \times C_{F_2}(r_1) = \langle r_1 \rangle \times \langle r_1 \rangle \tag{5.7}$$

and so a is conjugate to b in H if and only if $C_{F_2 \times F_2}(a)(w, 1) \cap H \neq 0$. This is of course true if and only if $(w, 1) \in H$, or equivalently if $w = 1$ in G, which is undecidable by the choice of G.

Consequently, the conjugacy problem is undecidable in H. □

Recall that every finitely presentable residually free group is a full subdirect prod-

uct of finitely many limit groups [32]:

$$G \leq D := L_1 \times \cdots \times L_n. \tag{5.8}$$

We shall write $\|g\|_G$ for the length of an element g in the usual word metric with respect to the generating set in G, and $\|g\|_D$ for the length of an element g in the usual word metric with respect to the generating set in D.

5.1 Preliminaries

Definition 5.1.1. A *polycyclic group* is a group G which has a subnormal series

$$1 = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_n = G \tag{5.9}$$

in which each H_{i+1}/H_i is cyclic.

Example 5.1.2. Finitely generated nilpotent groups are polycyclic. [37]

Definition 5.1.3. The *Hirsch length* of a polycyclic group is the number of infinite factors in the polycyclic series for that group.

Definition 5.1.4. Let G_1, G_2, Q be groups with homomorphisms

$$\alpha : G_1 \to Q \text{ and } \beta : G_2 \to Q. \tag{5.10}$$

The *fibre product* (or *pullback*) of G_1 and G_2 over Q is the following subgroup of $G_1 \times G_2$

$$G \times_Q H := \{(g_1, g_2) \ : \ \alpha(g_1) = \beta(g_2)\}. \tag{5.11}$$

The following well-known lemma implies that the subdirect product of two groups can be described as a fibre product of two groups, and vice versa.

Lemma 5.1.5 (Goursat's Lemma, [27])**.** *Let G_1, G_2 be two groups, with $H \leq G_1 \times G_2$. Let*

$$p_1 : G_1 \times G_2 \to G_1 \text{ and } p_2 : G_1 \times G_2 \to G_2 \tag{5.12}$$

be the natural projections of $G_1 \times G_2$ onto G_1, G_2, and let

$$i_1 : G_1 \to G_1 \times G_2 \text{ and } i_2 : G_2 \to G_1 \times G_2 \tag{5.13}$$

be the natural inclusions of G_1, G_2 into $G_1 \times G_2$.

There is a bijective correspondence between H and the quintuple

$$(p_1(H), p_2(H), i_1^{-1}(H \cap G_1), i_2^{-1}(H \cap G_2), \phi), \tag{5.14}$$

where $\phi : p_1(H)/i_1^{-1}(H \cap G_1) \to p_2(H)/i_2^{-1}(H \cap G_2)$ *is an isomorphism.*

The following lemma is necessary in a later proof, but is written here to avoid interrupting the flow of the main argument.

Lemma 5.1.6. *For any* $a_1, \ldots, a_k \in \mathbb{Z}$*, write* $d := gcd(a_1, \ldots, a_k)$*. Then there exists a matrix* $W \in GL(k, \mathbb{Z})$ *such that*

$$W \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{5.15}$$

and the entries of W *are all bounded above by a polynomial function of*

$$\beta_k := \max\{|a_1|, \ldots, |a_k|\}. \tag{5.16}$$

Proof. Bézout's lemma [8] states that, for any coprime $u, v \in \mathbb{Z}$, there exists a pair of integers (α_1, α_2) such that

$$\alpha_1 u + \alpha_2 v = 1 \tag{5.17}$$

and that the set $\{(\alpha_1 + zv, \alpha_2 + zu), z \in \mathbb{Z}\}$ provides all other solutions to this equation. In particular, we can assume without loss of generality that

$$|\alpha_1| \leq |v|. \tag{5.18}$$

Then

$$\begin{aligned} |\alpha_2| \cdot |v| + 1 &= |\alpha_2 v| + 1 \\ &= |\alpha_1 u|, \text{ by Equation 5.17} \\ &= |\alpha_1| \cdot |u| \\ &\leq |uv|, \text{ by Equation 5.18} \end{aligned} \tag{5.19}$$

which implies that $|\alpha_2| \leq |u|$.

This allows us to form the base of our induction on k. For $i \leq k$ write $d_i := gcd(a_1, \ldots, a_i)$. Note that $d_{i+1} = gcd(d_i, a_{i+1})$ and write $B_i := \max\{|a_1|, \ldots, |a_i|\}$.

There exist $x, y, z, t \in \mathbb{Z}$ such that

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} d_2 \\ 0 \end{pmatrix} \tag{5.20}$$

where

$$\begin{aligned} |x| = |d_2\alpha_1| \quad &\leq 2B_2, \\ |y| = |d_2\alpha_2| \quad &\leq 2B_2, \\ |z| = |\pm a_2/d_2| &\leq B_2, \\ |t| = |\mp a_1/d_2| &\leq B_2. \end{aligned} \tag{5.21}$$

Now suppose that there exists a matrix $W_i \in GL_i(\mathbb{Z})$ with entries which are bound by a polynomial function of B_i. Then set

$$W_{i+1} := \left(\begin{array}{c|ccc|c} x & 0 & \cdots & 0 & y \\ \hline 0 & & & & 0 \\ \vdots & & \mathbb{I}_i & & \vdots \\ 0 & & & & 0 \\ \hline z & 0 & \cdots & 0 & t \end{array}\right) \left(\begin{array}{ccc|c} & & & 0 \\ & W_i & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & 1 \end{array}\right) \tag{5.22}$$

where $\mathbb{I}_i$ is the identity matrix in $GL_i(\mathbb{Z})$, and x, y, z, t are provided by 5.20 as in the base case.

Multiplying these matrices together gives

$$W_{i+1} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{i+1} \end{pmatrix} = \begin{pmatrix} d_{i+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{5.23}$$

and since the entries of W_i are bounded above by a polynomial function of B_{i+1} then the entries of W_{i+1} are also bound by a polynomial function of B_{i+1}. □

Definition 5.1.7. Let $n \geq 2$. A subgroup $G < L_1 \times \ldots \times L_n$ is said to be *virtually surjective on pairs*, if for all $i < j \in \{1, \ldots, n\}$, the projection $p_{i,j} : G \to L_i \times L_j$ has finite index in $L_i \times L_j$. Groups which are virtually surjective on pairs are said to satisfy the *VSP property*.

It was shown in [13, Corollary 4.3] that finitely presented residually free groups satisfy the VSP property.

Let $G < D$ be a finitely presentable residually free group. It is important that throughout this section we choose D so that G is a full subdirect product as discussed at the beginning of this chapter. Suppose that

$$A = [\mathbf{a}_1, \ldots, \mathbf{a}_m] \text{ and } B = [\mathbf{b}_1, \ldots, \mathbf{b}_m] \tag{5.24}$$

are two lists of elements in G such that $\mathbf{a}_j$ is conjugate to $\mathbf{b}_j$ in G for each $j = 1, \ldots, m$. We seek an upper bound on the length of a smallest conjugator, as a function of the lengths of the input elements of the lists A and B. For each $j \in \{1, \ldots, m\}$, write $\mathbf{a}_j$ and $\mathbf{b}_j$ as elements of G embedded in D:

$$\mathbf{a}_j = (a_j^{(1)}, \ldots, a_j^{(n)}) \text{ and } \mathbf{b}_j = (b_j^{(1)}, \ldots, b_j^{(n)}). \tag{5.25}$$

Analysing this componentwise, for each i we have:

$$a_j^{(i)} \sim b_j^{(i)} \ \forall j \tag{5.26}$$

in $p_i(G) \cap L_i$, which is the multiple conjugacy search problem in the limit group $p_i(G) \cap L_i$. For each $i = 1, \ldots, n$ we can find $x^{(i)} \in L_i$ such that $(x^{(i)})^{-1} a_j^{(i)} x^{(i)} = b_j^{(i)}$ for all $j = 1, \ldots, m$ using Theorem 4.3.5 such that $\|x^{(i)}\|_G$ is bounded by a linear function of $\max\{\|a_j^{(i)}\|_D, \|b_j^{(i)}\|_D\}$. Use these $x^{(i)}$ to define $\mathbf{x} := (x^{(1)} \ldots x^{(n)}) \in D$. Any other element which conjugates $a_j^{(i)}$ to $b_j^{(i)}$ can be written as $z^{(i)} x^{(i)}$, where

$$z^{(i)} \in \bigcap_j C_{L_i}(a_j^{(i)}), \tag{5.27}$$

and so any element which conjugates $\mathbf{a}_j$ to $\mathbf{b}_j$ for all j can be written as $\mathbf{zx}$, where

$$\mathbf{z} \in \prod_i \bigcap_j C_{L_i}(a_j^{(i)}) = \bigcap_j C_D(\mathbf{a}_j) < D. \tag{5.28}$$

Since D is a direct product of limit groups then the elements of the generating set Z of $\bigcap_j C_D(\mathbf{a}_j)$ have a length bound which is linear with respect to $\|\mathbf{a}\|_D$ by Corollary 4.2.3. Likewise, the size of the set Z has a constant bound which depends on the choice of limit groups.

Lemma 5.1.8. *Let G be a finitely presented residually free group. There is a constant $\mathcal{C}$ such that for any two lists in G*

$$A = [\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m] \text{ and } B = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m] \tag{5.29}$$

in which $\boldsymbol{a}_i$ is conjugate to $\boldsymbol{b}_i$ for $i = 1, \ldots, m$, the length m of A and B is bounded above by $\mathcal{C}$.

Proof. The group G has a canonical embedding into a direct product D of limit groups satisfying the virtual surjection to pairs (VSP) property. The number $\mathcal{N}$ of non-abelian limit groups in this direct product depends only on G.

In each limit group factor L_i of D, the centraliser of the projection of A is one of the following.

- L_i, if A maps entirely into the centre of L_i. Note that L_i is the centraliser in L_i of $\{1\}$.
- A cyclic subgroup C if the image of A in L_i is not central but consists of a set of mutually commuting elements. In this case C is the centraliser in L_i of any non-central element in the set.
- $\{1\}$ otherwise. In this case $\{1\}$ is the centraliser in L_i of any pair of non-commuting elements in the image of A.

It follows that the centraliser in D of any list A is equal to the centraliser of some sub-list consisting of at most $2\mathcal{N}$ elements. Thus the multiple conjugacy length problem for G reduces to the case of lists of at most $2\mathcal{N}$ elements. This is the required universal bound for G. □

Lemma 5.1.9. *Let A, B be conjugate lists in $G \leq L_1 \times \cdots \times L_n$ as described in equation (5.24). Then we can assume that, for each $j = 1, \ldots, n$, the centraliser $C_D(\boldsymbol{a}_j)$ is a free abelian group.*

Proof. Choose a generating set X for G. The centraliser of $p_i(\mathbf{a}_j)$ is of course abelian, unless $p_i(\mathbf{a}_j) = 1$, in which case $C_{L_i}(p_i(\mathbf{a}_j)) = L_i$, and this is not necessarily abelian. However we can project away from this limit group L_i. Assume, without loss of generality, that $i = 1$. Define the epimorphism $q : G \to \overline{G}$ where

$$\overline{G} = \frac{G \cdot L_1}{L_1} \subseteq L_2 \times \cdots \times L_n. \tag{5.30}$$

If $\overline{g}\mathbf{a}_j\overline{g}^{-1} = \mathbf{b}$ then for any $g \in G$ such that $\overline{g} = q(g)$, it is easy to see that $g\mathbf{a}g^{-1} = \mathbf{b}$.

We have to be careful: since $\overline{G}$ is a homomorphic image of G, it is not necessarily finitely presented. However, it inherits the VSP property from G, and is therefore finitely presentable [14]. □

5.2 Multiple conjugacy search problem using the word metric in D

We use the property that D/N, where $N = \prod_{i=1}^{n}(L_i \bigcap G)$, is virtually nilpotent (by [13, Theorem 4.2]) to produce the following chain of subgroups:

$$G = \Gamma_0 \lhd \Gamma_1 \lhd \ldots \lhd \Gamma_h \leq D \tag{5.31}$$

where h is the difference between the Hirsch lengths of $\frac{D}{N}$ and $\frac{G}{N}$ (recall Definition 5.1.3), and Γ_h has finite index in D.

Lemma 5.2.1. *Let G be a finitely presented residually free group with conjugate lists A, B as described in equation (5.24). Suppose that $\boldsymbol{x} \in D$ is a conjugator of A, B in D. Then there exists an element $\boldsymbol{c} \in \bigcap_j C_D(\boldsymbol{a}_j)$ such that $\boldsymbol{cx} \in \Gamma_0$, and that the length $\|\boldsymbol{c}\|_D$ is bounded by a polynomial over* $\max\{\|\boldsymbol{a}_j\|_D, \|\boldsymbol{b}_j\|_D\}_j$.

Proof. We use induction on the length of this subgroup chain. There are two cases to consider because by [13, Corollary 8.2] the quotient groups $\frac{\Gamma_{k+1}}{\Gamma_k}$ are either finite or infinite cyclic. We deal with each of these in turn.

Finite quotient.

We begin with the case of the finite quotient D/Γ_h. This same argument can be used whenever Γ_{k+1}/Γ_k is finite.

Let $Z = \{\mathbf{r}_1, \ldots, \mathbf{r}_\ell\}$ be the generating set of $\bigcap_j C_D(\mathbf{a}_j)$. We want to find $\mathbf{c} \in \bigcap_j C_D(\mathbf{a}_j)$ such that $\mathbf{cx} \in \Gamma_h$. Equivalently, the cosets $\mathbf{c}\Gamma_h = \mathbf{x}\Gamma_h$ in $\frac{D}{\Gamma_h}$. Since Γ_h has finite index in D we can form the finite coset graph $\mathcal{X}$ of Γ_h in D with edges labelled by $\mathbf{r}_i$ for $i = 1, \ldots, \ell$. There is a geodesic path in $\mathcal{X}$ from $1\Gamma_h$ to $\mathbf{x}\Gamma_h$. Since $\mathcal{X}$ is a finite graph, the length of this path is bounded by the size of D/Γ_h, and the number of such paths is bounded by a constant $\mathcal{C} \in \mathbb{N}$ which is determined by D and Γ_h (and thus is determined by G). This gives an upper bound on the length of an element $\mathbf{c}$ in $\bigcap_j C_D(\mathbf{a}_j)$ such that $\mathbf{c}\Gamma_h = \mathbf{x}\Gamma_h$:

$$\|\mathbf{c}\|_D \leq \mathcal{C} \cdot \max\{\|\mathbf{r}_i\|_D\}_{i=1}^{\ell}, \tag{5.32}$$

which is a linear function of $\max\{\|\mathbf{a}_j\|_D, \|\mathbf{b}_j\|_D\}_j$.

Infinite cyclic quotient.

Suppose inductively that we have

1. $\mathbf{x}_{k+1} \in \Gamma_{k+1}$ with $\mathbf{x}_{k+1}^{-1}\mathbf{a}_j\mathbf{x}_{k+1} = \mathbf{b}_j$ for all j, with $\|\mathbf{x}_{k+1}\|_D$ bounded above by a function which is polynomial over $\max\{\|\mathbf{a}_j\|_D, \|\mathbf{b}_j\|_D\}_j$;
2. A set $Z_{k+1} := \{\mathbf{s}_1, \ldots, \mathbf{s}_\ell\}$ of generators for $\bigcap_j C_{\Gamma_{k+1}}(\mathbf{a}_j)$, such that $\|\mathbf{s}_i\|_D$ is bounded by a function which is a polynomial over $\max\{\|\mathbf{a}_j\|_D, \|\mathbf{b}_j\|_D\}_j$.

We want to find an element $\mathbf{c}_{k+1}$ of polynomial length in Z_{k+1} such that

$$\mathbf{c}_{k+1}G_k = \mathbf{x}_{k+1}G_k \tag{5.33}$$

in $\frac{\Gamma_{k+1}}{\Gamma_k} \cong \mathbb{Z}$, so that $\mathbf{c}_{k+1}^{-1}\mathbf{x}_{k+1}$ is an element of Γ_k which conjugates $\mathbf{a}_j$ to $\mathbf{b}_j$ for all j. Similarly, we want a new generating set Z_k for the centraliser in Γ_k of the set $\{\mathbf{a}_j\}_{j=1}^n$. Note that

$$C_{\Gamma_k}(\mathbf{a}_j) \leq C_{\Gamma_{k+1}}(\mathbf{a}_j) \tag{5.34}$$

for all j.

Since $\Gamma_{k+1} = \langle \mathbf{t}_k \rangle \ltimes \Gamma_k$, we can write $\mathbf{x}_{k+1} = \mathbf{t}_k^{\alpha} \mathbf{x}_k$. We can assume that $\mathbf{t}$ is a generator for Γ_{k+1}, and define a homomorphism $\phi : \Gamma_{k+1} \to \mathbb{Z}$ which maps $\mathbf{t}^i$ to i for all $i \in \mathbb{Z}$, and maps every other generating element to 0. Write $n_i := \phi(\mathbf{z}_i)$ for each $\mathbf{z}_i \in Z_{k+1}$, and let $|Z_{k+1}| = \ell'$.

If $n_i = 0$ for $i = 1, \ldots, \ell'$ then $\mathbf{z}_1, \ldots, \mathbf{z}_{\ell'} \in \Gamma_k$ so $\mathbf{x}_{k+1}$ is also an element of G_k. Set $Z_k := Z_{k+1}$ and set $\mathbf{x}_k := \mathbf{x}_{k+1}$. Otherwise, assume that at least one $n_i \neq 0$.

Let $d_i := gcd(n_1, \ldots, n_i)$. Note that $|d_i| \leq \max\{|n_1|, \ldots, |n_i|\}$, and that $|n_i|$ is a linear function of $\phi(\mathbf{x}_{k+1})$ by Corollary 4.2.3 – and so a polynomial function of $\max\{\|\mathbf{a}_j\|_D, \|\mathbf{b}_j\|_D\}_j$ by the inductive hypothesis. Then

$$\begin{aligned} \alpha &= \phi(\mathbf{x}_{k+1}) \\ &= \phi(\mathbf{z}_1^{\lambda_1} \ldots \mathbf{z}_{\ell'}^{\lambda_{\ell'}}) \\ &= \lambda_1 n_1 + \cdots + \lambda_{\ell'} n_{\ell'}, \text{ by Corollary 4.2.3} \\ &= \mu d_{\ell'} \end{aligned} \tag{5.35}$$

for some $\mu \in \mathbb{Z}$.

We can apply a matrix $W \in GL_{\ell'}(\mathbb{Z})$ to the column vector

$$\mathbf{Z_{k+1}} := \begin{pmatrix} \mathbf{z}_1 \\ \vdots \\ \mathbf{z}_{\ell'} \end{pmatrix} \tag{5.36}$$

to get

$$\mathbf{Z'_{k+1}} := \begin{pmatrix} \mathbf{z}'_1 \\ \vdots \\ \mathbf{z}'_{\ell'} \end{pmatrix} \tag{5.37}$$

such that

$$\begin{pmatrix} n'_1 \\ n'_2 \\ \vdots \\ n'_{\ell'} \end{pmatrix} = \begin{pmatrix} \phi(\mathbf{z}'_1) \\ \phi(\mathbf{z}'_2) \\ \vdots \\ \phi(\mathbf{z}'_{\ell'}) \end{pmatrix} = \phi \left(W \begin{pmatrix} \mathbf{z}_1 \\ \mathbf{z}_2 \\ \vdots \\ \mathbf{z}_{\ell'} \end{pmatrix} \right) = W \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_{\ell'} \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{5.38}$$

By Lemma 5.1.6 the entries of the matrix W are bounded above by a polynomial function of $\max\{|n_i|\}_i$.

Set

$$\mathbf{x}_k := (\mathbf{z}'_1)^{-\phi(\mathbf{x}_{k+1})/d} \cdot \mathbf{x}_{k+1}. \tag{5.39}$$

Then $\phi(\mathbf{x}_k) = 0$ and so $\mathbf{x}_k \in \Gamma_k$.

We claim that $\{\mathbf{z}'_2, \ldots, \mathbf{z}_{\ell'}\}$ forms a generating set Z_k for $C_{\Gamma_k}(\mathbf{a}_j)$.

Let $\mathbf{c} \in C_{\Gamma_k}(\mathbf{a}_j)$. Then $\phi(\mathbf{c}) = 0$, and $\mathbf{c} \in C_{\Gamma_{k+1}}(\mathbf{a}_j)$, so there exist $\alpha_1, \ldots, \alpha_{\ell'} \in \mathbb{Z}$ such that

$$\mathbf{c} = \alpha_1 \mathbf{z}_1 + \cdots + \alpha_{\ell'} \mathbf{z}_{\ell'}. \tag{5.40}$$

Write

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{\ell'} \end{pmatrix} = W^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{\ell'} \end{pmatrix}. \tag{5.41}$$

Then

$$\mathbf{c} = \beta_1 \mathbf{z}'_1 + \cdots + \beta_{\ell'} \mathbf{z}'_{\ell'}. \tag{5.42}$$

So

$$0 = \phi(\mathbf{c}) = \phi(\beta_1(\mathbf{z}'_1) + \cdots + \beta_\ell(\mathbf{z}'_{\ell'})) = \beta_1 d_{\ell'} \tag{5.43}$$

by Equation 5.38, which implies that $\beta_1 = 0$, and so $\mathbf{c} \in \mathrm{span}(\mathbf{z}'_2, \ldots, \mathbf{z}'_{\ell'})$. Hence Z_k is a generating set for $C_{\Gamma_k}(\mathbf{a}_j)$ whose elements are length-bound by a polynomial over

$$\max\{\|\mathbf{a}_j\|_D, \|\mathbf{b}_j\|_D\}_j, \tag{5.44}$$

which completes the induction. □

Induction on the Hirsch length does not quite yield a conjugator in G. Instead we have found a conjugator in G_0, which is a finite-index subgroup of G. The following lemma, which applies to finitely presented residually free groups, provides a partial solution to the multiple conjugacy search problem in G, although there is still the issue of subgroup distortion to consider.

Definition 5.2.2. A group G is said to have the *unique roots property* if, for any integer $n > 1$, if $x, y \in G$ with $x^n = y^n$ then $x = y$.

Lemma 5.2.3. *Limit groups have the unique roots property.*

Proof. Let L be a limit group, and let $n \in \mathbb{N}$ such that $x^n = y^n$ for some $x, y \in L$. Let $S = \{x, y, x^n, y^n\} \subseteq L$. Since L is fully residually free, there is a monomorphism ϕ into a free group F which is injective when restricted to S. Thus

$$x^n = y^n \Rightarrow \phi(x^n) = \phi(y^n) \tag{5.45}$$

and since F is free then it clearly satisfies the unique roots property, so that

$$\phi(x^n) = \phi(y^n) \Rightarrow \phi(x) = \phi(y). \tag{5.46}$$

The injectivity of ϕ then implies that

$$\phi(x) = \phi(y). \tag{5.47}$$

□

Lemma 5.2.4. *Let H be a subgroup of index $d < \infty$ in a finitely generated group G. Assume that H has a polynomial multiple conjugacy length function of degree n. Assume also that G has the unique roots property. Then G has a multiple conjugacy length function which is polynomial of degree n.*

Proof. Let $R = \{r_1, \ldots, r_d\}$ be a right transversal for H in G, and let $N \triangleleft G$ be the core of H: $N = \bigcap_{j=1}^{d} r_j^{-1} H r_j$. Then N is the kernel of the coset representation $G \to S_d$, so has index dividing $d!$.

Suppose that $A = [a_1, \ldots, a_m]$ and $B = [b_1, \ldots, b_m]$ are conjugate lists of m elements in G – say $B = g^{-1}Ag$ with $g \in G$. Then $A^{d!} = [a_1^{d!}, \ldots, a_m^{d!}]$ and $B^{d!} = [b_1^{d!}, \ldots, b_m^{d!}]$ are lists in $N < H$ and $B^{d!} = g^{-1}A^{d!}g$. Now $g = hr_j$ for some $h \in H$ and some $j = 1, \ldots, d$. Then $A^{d!}$ and $C := r_j B^{d!} r_j^{-1}$ are lists of m elements of $N < H$ which are conjugate in H: $C = h^{-1}A^{d!}h$.

Suppose that f is a polynomial multiple conjugacy length function for H. Then there is an element $x \in H$ such that $C = x^{-1}A^{d!}x$ and

$$\|x\|_X \leq f(\|A^{d!}\|_X + \|C\|_X) \leq f(d!(\|A\|_X + \|B\|_X) + 2Mm), \tag{5.48}$$

where $M := \max\{\|r_j\|_X;\ j = 1, \ldots, d\}$.

Now define $y := xr_j \in G$. Then $y^{-1}A^{d!}y = r_j^{-1}Cr_j = B^{d!}$. It follows easily from the unique roots property that $y^{-1}Ay = B$. Moreover,

$$\|y\|_X \leq \|r_j\|_X + \|x\|_X \leq M + f(d!(\|A\|_X + \|B\|_X) + 2Mm), \tag{5.49}$$

and the right-hand side of this inequality is polynomial of degree n. Finally, note that m is bounded by a constant, by Lemma 5.1.8. □

5.3 Subgroup distortion

Theorem 5.3.1. *Let A, B, Q be finitely generated groups with Q virtually nilpotent of class c. Let $\alpha : A \to Q$, $\beta : B \to Q$ be epimorphisms, and*

$$G = \{(a, b) \in A \times B \mid \alpha(a) = \beta(b)\} \tag{5.50}$$

the fibre product of α and β. Then G is finitely generated, and the distortion of G in $A \times B$ is polynomial of degree at most $c + 2$.

Proof. Since finite-index subgroups are undistorted, we can replace Q by a nilpotent subgroup Q_0 of finite index, and each of A, B, G by the preimage of Q_0, without effectively changing the problem. Hence we may assume without loss of generality that Q is nilpotent of class c.

Let

$$p_A : A \times B \to A \text{ and } p_B : A \times B \to B \tag{5.51}$$

be the canonical projections. Since A and B are finitely generated and $p_A(G) = A$, $p_B(G) = B$, there is a finite subset X of G such that $p_A(X)$ generates A and $p_B(X)$ generates B. Hence also $\alpha(p_A(X)) = \beta(p_B(X))$ generates Q. Let $F = F(X)$ denote the free group with basis X and $\phi : F \to Q$ the epimorphism induced by the map $X \to Q$. Since Q is finitely generated and nilpotent, it is finitely presentable, so that the kernel of ϕ is the normal closure in $F(X)$ of some finite subset R. In other words, $\langle X|R\rangle$ is a finite presentation for Q. By [25, Theorem B], this presentation has an (Area,FL)-pair of the form (n^{c+1}, n). In other words, there are polynomials $P(n), L(n)$ of degrees $c+1, 1$ respectively, such that, if W is a word of length n in $X \cup X^{-1}$ representing an element of $\mathrm{Ker}(\phi)$, then there is a sequence of words

$$W = W_0, W_1, \ldots, W_N = 1 \tag{5.52}$$

with $N \leq P(n)$ and $|W_j| \leq L(n)$ for each j, such that W_{j+1} is either freely equal to W_j, or $W_j \equiv guh$, $W_{j+1} \equiv gvh$ as words, with uv^{-1} equal to a cyclic conjugate of a relator or its inverse.

It follows that there is, for any such W, an equation in $F(X)$ of the form

$$W =_{F(X)} \prod_{j=1}^{N} g_j r_j^{\varepsilon(j)} g_j^{-1}, \tag{5.53}$$

with $N \leq P(n)$, and for each j: $r_j \in R$, $\varepsilon(j) = \pm 1$ and $|g_j| \leq L(n) + M$, where M is the constant $M := \max\{|r|; r \in R\}$.

We now define $\pi_A : F(X) \to A$, $\pi_B : F(X) \to B$ to be the homomorphisms induced from $p_A|_X : X \to A$, $p_B|_X : X \to B$ respectively, and Y to be the finite subset

$$Y := \{(p_A(x), p_B(x)); x \in X\} \cup \{(1, \pi_B(r)); r \in R\} \tag{5.54}$$

of G. We claim that G is generated by Y, and that the distortion of G (with respect to Y) in $A \times B$ (with respect to the generating set $(p_A(X) \times \{1\}) \cup (\{1\} \times p_B(X))$) is polynomial of degree at most $c + 2$.

To see this, suppose that $h \in G$ is an element that can be expressed as a word of length n in the generators of $A \times B$. Then there are words W_1, W_2 in $X \cup X^{-1}$ such

that $n = |W_1| + |W_2|$ and

$$h = (\pi_A(W_1), \pi_B(W_2)). \tag{5.55}$$

Then $W := W_1^{-1}W_2$ is a word of length n in $X \cup X^{-1}$ representing an element of $\mathrm{Ker}(\phi)$. Hence W has an expression $\prod_j g_j r_j^{\varepsilon(j)} g_j^{-1}$ as above. Then

$$h_1 := (\pi_A(W_1), \pi_B(W_1)) \in G \tag{5.56}$$

can be expressed as a word of length $|W_1| \leq n$ in $Y \cup Y^{-1}$, and $h_2 := (1, W) \in G$ can be expressed as a word

$$h_2 = \prod_{j=1}^{N} (\pi_A(g_j), \pi_B(g_j)) \cdot (1, r_j)^{\varepsilon(j)} \cdot (\pi_A(g_j), \pi_B(g_j))^{-1} \tag{5.57}$$

of length at most $P(n)(2L(n)+2M+1)$ in $Y \cup Y^{-1}$. Hence the given element $h = h_1 h_2$ of G can be expressed as a word of length at most

$$T(n) := P(n)(2L(n) + 2M + 1) + L(n) \tag{5.58}$$

in $Y \cup Y^{-1}$ Since $T(n)$ is a polynomial in n of degree $c + 2$, the result follows.

□

Corollary 5.3.2. *Let G be a finitely presentable residually free group. Then G can be embedded with polynomial distortion into a direct product of limit groups.*

Proof. By [13] there is a direct product $D = L_0 \times \cdots \times L_n$ of limit groups and an embedding $G \hookrightarrow D$ such that: L_0 is abelian and L_j is non-abelian for each $j > 0$, $|L_0 : G \cap L_0| < \infty$, for each $0 \leq j \leq n$ the projection $p_j : G \to L_j$ is surjective, and for each $0 \leq j < k \leq n$ the projection $p_{jk} : D \to L_j \times L_k$ maps G onto a finite-index subgroup of $L_j \times L_k$. Since L_j is normal in D, it follows that $L_j \cap G$ is normal in L_j for each j. It also follows (see for example [13]) that $L_j/(L_j \cap G)$ is virtually nilpotent of class at most $n - 2$, for each j (provided that $n \geq 2$ so that the statement makes sense). Finally, note that the image $\overline{G}$ of G in $\overline{D} := L_0 \times \cdots \times L_{n-1}$ also satisfies the conditions of [13], and so is finitely presentable.

We use these observations to prove by induction on n that the distortion of G in D is polynomial of degree at most $n!/2$ when $n \geq 2$. When $n \leq 2$ then the above remarks show that $|D : G| < \infty$, so G is undistorted. In particular, this covers the base case $n = 2$ of the induction.

Suppose then that $n \geq 3$ and that the desired result holds in direct products of fewer factors. Then in particular the distortion of $\overline{G}$ in $\overline{D}$ is polynomial of degree at most $(n-1)!/2$. Taking direct products with L_n, the distortion of $\overline{G} \times L_n$ in $\overline{D} \times L_n = D$ is polynomial of degree at most $(n-1)!/2$. So it suffices to show that the distortion of

G in $\overline{G} \times L_n$ is polynomial of degree at most n. But this follows from Theorem 5.3.1, together with the observation that G is a fibre-product of epimorphisms $\overline{G} \to Q$ and $L_n \to Q$ where $Q := L_n/(L_n \cap G)$ is virtually nilpotent of class at most $n-2$.

□

Chapter 6

Epilogue

We have found conjugacy length bounds for several classes of groups: relatively hyperbolic groups, limit groups, and finitely presented residually free groups. There are opportunities to build upon this work – for example, this thesis does not provide a time bound for solving the (multiple) conjugacy search problem for the groups which are featured. Further investigation could provide algorithms for solving such problems.

The multiple conjugacy search problem for relatively hyperbolic groups is conspicuously missing from this thesis. Bridson and Howie [12] showed that the multiple conjugacy search problem for hyperbolic groups has a linear asymptotic bound, and their argument is based on the Cayley graph of the hyperbolic groups. The problem with using a similar argument for relatively hyperbolic groups is that the argument relies on putting a finite upper bound on the size of the centralisers by looking at the action of certain elements on the Cayley graph to see if the centralisers intersect at a finite number of points. However if we look at the action of a relatively hyperbolic group on $\widehat{\Gamma}$ then a ball of bounded radius in $\widehat{\Gamma}$ contains an infinite number of vertices.

Some other questions arising from this thesis: Are the conjugacy length functions for this thesis optimal? In terms of applications to group-based cryptography, can we establish a lower bound for groups which are solvable, but deemed to be "hard" to solve?

Bibliography

[1] Emina Alibegović and Mladen Bestvina. Limit groups are CAT(0). *J. London Math. Soc. (2)*, 74(1):259–272, 2006.

[2] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, 6(3-4):287–291, 1999.

[3] Benjamin Baumslag. Residually free groups. *Proc. London Math. Soc. (3)*, 17:402–418, 1967.

[4] G. Baumslag, C. F. Miller, III, and H. Short. Unsolvable problems about small cancellation and word hyperbolic groups. *Bull. London Math. Soc.*, 26(1):97–101, 1994.

[5] Gilbert Baumslag, Martin R. Bridson, Charles F. Miller, III, and Hamish Short. Finitely presented subgroups of automatic groups and their isoperimetric functions. *J. London Math. Soc. (2)*, 56(2):292–304, 1997.

[6] Gilbert Baumslag, Martin R. Bridson, Charles F. Miller, III, and Hamish Short. Fibre products, non-positive curvature, and decision problems. *Comment. Math. Helv.*, 75(3):457–477, 2000.

[7] Mladen Bestvina and Mark Feighn. Notes on Sela's work: limit groups and Makanin-Razborov diagrams. In *Geometric and cohomological methods in group theory*, volume 358 of *London Math. Soc. Lecture Note Ser.*, pages 1–29. Cambridge Univ. Press, Cambridge, 2009.

[8] Etienne Bézout. *General theory of algebraic equations*. Princeton University Press, Princeton, NJ, 2006. Translated from the 1779 French original by Eric Feron.

[9] Robert Bieri. *Homological dimension of discrete groups*. Mathematics Department, Queen Mary College, London, 1976. Queen Mary College Mathematics Notes.

[10] B. H. Bowditch. Relatively hyperbolic groups. *Internat. J. Algebra Comput.*, 22(3):1250016, 66, 2012.

[11] Martin R. Bridson and André Haefliger. *Metric spaces of non-positive curvature*, volume 319 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[12] Martin R. Bridson and James Howie. Conjugacy of finite subsets in hyperbolic groups. *Internat. J. Algebra Comput.*, 15(4):725–756, 2005.

[13] Martin R. Bridson, James Howie, Charles F. Miller, III, and Hamish Short. Subgroups of direct products of limit groups. *Ann. of Math. (2)*, 170(3):1447–1467, 2009.

[14] Martin R. Bridson, James Howie, Charles F. Miller, III, and Hamish Short. On the finite presentation of subdirect products and the nature of residually free groups. *Amer. J. Math.*, 135(4):891–933, 2013.

[15] David J. Buckley and Derek F. Holt. The conjugacy problem in hyperbolic groups for finite lists of group elements. unpublished.

[16] Inna Bumagin. The conjugacy problem for relatively hyperbolic groups. *Algebr. Geom. Topol.*, 4:1013–1040, 2004.

[17] Inna Bumagin. On definitions of relatively hyperbolic groups. In *Geometric methods in group theory*, volume 372 of *Contemp. Math.*, pages 189–196. Amer. Math. Soc., Providence, RI, 2005.

[18] Steve Burnett and Stephen Paine. *The RSA Security's Official Guide to Cryptography*. McGraw-Hill, Inc., New York, NY, USA, 2001.

[19] John Crisp, Eddy Godelle, and Bert Wiest. The conjugacy problem in subgroups of right-angled Artin groups. *J. Topol.*, 2(3):442–460, 2009.

[20] François Dahmani. Combination of convergence groups. *Geom. Topol.*, 7:933–963 (electronic), 2003.

[21] M. Dehn. Über unendliche diskontinuierliche Gruppen. *Math. Ann.*, 71(1):116–144, 1911.

[22] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.

[23] David B. A. Epstein, James W. Cannon, Derek F. Holt, Silvio V. F. Levy, Michael S. Paterson, and William P. Thurston. *Word processing in groups*. Jones and Bartlett Publishers, Boston, MA, 1992.

[24] Benson Farb. Relatively hyperbolic groups. *Geom. Funct. Anal.*, 8(5):810–840, 1998.

[25] S. M. Gersten, D. F. Holt, and T. R. Riley. Isoperimetric inequalities for nilpotent groups. *Geom. Funct. Anal.*, 13(4):795–814, 2003.

[26] S. M. Gersten and H. B. Short. Small cancellation theory and automatic groups. *Invent. Math.*, 102(2):305–334, 1990.

[27] Edouard Goursat. Sur les substitutions orthogonales et les divisions régulières de l'espace. *Ann. Sci. École Norm. Sup. (3)*, 6:9–102, 1889.

[28] M. Gromov. Hyperbolic groups. In *Essays in group theory*, volume 8 of *Math. Sci. Res. Inst. Publ.*, pages 75–263. Springer, New York, 1987.

[29] J. Hughes and A. Tannenbaum. Length-based attacks for certain group based encryption rewriting systems, 2002.

[30] Ronghui Ji, Crichton Ogle, and Bobby Ramsey. Relatively hyperbolic groups, rapid decay algebras and a generalization of the Bass conjecture. *J. Noncommut. Geom.*, 4(1):83–124, 2010. With an appendix by Ogle.

[31] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. I. Irreducibility of quadratic equations and Nullstellensatz. *J. Algebra*, 200(2):472–516, 1998.

[32] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. II. Systems in triangular quasi-quadratic form and description of residually free groups. *J. Algebra*, 200(2):517–570, 1998.

[33] Olga Kharlampovich and Alexei Myasnikov. Elementary theory of free non-abelian groups. *Journal of Algebra*, 302(2):451 – 552, 2006.

[34] Olga Kharlampovich and Alexei Myasnikov. Elementary theory of free non-abelian groups. *J. Algebra*, 302(2):451–552, 2006.

[35] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In *Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA)*, volume 1880 of *Lecture Notes in Comput. Sci.*, pages 166–183. Springer, Berlin, 2000.

[36] Gerasim Kokarev. On geodesic homotopies of controlled width and conjugacies in isometry groups. to appear.

[37] John C. Lennox and Derek J. S. Robinson. *The theory of infinite soluble groups*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, Oxford, 2004.

[38] Hai-Ning Liu, C. Wrathall, and Kenneth Zeger. Efficient solution of some problems in free partially commutative monoids. *Inform. and Comput.*, 89(2):180–198, 1990.

[39] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Classics in Mathematics. Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition.

[40] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial group theory*. Dover Publications Inc., Mineola, NY, second edition, 2004. Presentations of groups in terms of generators and relations.

[41] K. A. Mihaĭlova. The occurrence problem for direct products of groups. *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958.

[42] Charles F. Miller, III. *On group-theoretic decision problems and their classification*. Princeton University Press, Princeton, N.J., 1971. Annals of Mathematics Studies, No. 68.

[43] Charles F. Miller, III. Decision problems for groups—survey and reflections. In *Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989)*, volume 23 of *Math. Sci. Res. Inst. Publ.*, pages 1–59. Springer, New York, 1992.

[44] A. G. Myasnikov and V. N. Remeslennikov. Exponential groups. II. Extensions of centralizers and tensor completion of CSA-groups. *Internat. J. Algebra Comput.*, 6(6):687–711, 1996.

[45] Denis Osin. Small cancellations over relatively hyperbolic groups and embedding theorems. *Ann. of Math. (2)*, 172(1):1–39, 2010.

[46] Denis V. Osin. Relatively hyperbolic groups: intrinsic geometry, algebraic properties, and algorithmic problems. *Mem. Amer. Math. Soc.*, 179(843):vi+100, 2006.

[47] V. N. Remeslennikov. $\exists$-free groups. *Sibirsk. Mat. Zh.*, 30(6):193–197, 1989.

[48] E. Rips. Subgroups of small cancellation groups. *Bull. London Math. Soc.*, 14(1):45–47, 1982.

[49] Zlil Sela. Diophantine geometry over groups. I. Makanin-Razborov diagrams. *Publ. Math. Inst. Hautes Études Sci.*, 93:31–105, 2001.

[50] Jean-Pierre Serre. Cohomologie des groupes discrets. *C. R. Acad. Sci. Paris Sér. A-B*, 268:A268–A271, 1969.

[51] Jean-Pierre Serre. *Trees*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation.

[52] John Stallings. A finitely presented group whose 3-dimensional integral homology is not finitely generated. *Amer. J. Math.*, 85:541–543, 1963.

[53] Andrzej Szczepański. Relatively hyperbolic groups. *Michigan Math. J.*, 45(3):611–618, 1998.

[54] C. T. C. Wall. Finiteness conditions for CW-complexes. *Ann. of Math. (2)*, 81:56–69, 1965.

[55] Henry Wilton. Hall's theorem for limit groups. *Geom. Funct. Anal.*, 18(1):271–303, 2008.